Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	File Nos.
GU HOLDINGS INC.,	)	
EDGE CABLE HOLDINGS USA, LLC	)	SCL-LIC-20170421-00012;
and	)	SCL-AMD-20171227-00025;
PACIFIC LIGHT DATA	)	SCL-STA-20180907-00033;
COMMUNICATION CO. LTD.	)	SCL-STA-20190327-00011;
	)	SCL-STA-20190906-00032;
Application for a License to Construct, Land,	)	SCL-STA-20200129-00006;
and Operate an Undersea Fiber Optic Cable	)	SCL-STA-20200313-00014;
Connecting the United States, Hong Kong,	)	SCL-STA-20200402-00015.
Taiwan, and the Philippines.	)	

Executive Branch Recommendation for a Partial Denial and Partial Grant of the Application for a Submarine Cable Landing License for the Pacific Light Cable Network (PLCN)

TABLE OF CONTENTS

I. Introduction

Interested Executive Branch agencies[1] submit this recommendation to the Federal Communications Commission (FCC or Commission) that it partially deny the Pacific Light Cable Network (PLCN) cable landing license application with respect to PLCN's connection to Hong Kong and with respect to PLCN's foreign owners, Hong Kong-based Pacific Light Data Communication Co. Ltd. and China-based ultimate parent entity Dr. Peng Telecom & Media Group Co., Ltd. The Executive Branch recommends that the Commission partially grant the license application for PLCN's U.S. owners and for PLCN's connections between the United States, Taiwan, and the Philippines, if prior to the Commission issuing an order, PLCN's U.S. owners reach final agreements with the Departments of Justice (DOJ), Homeland Security (DHS), and Defense (DOD) on specific mitigation measures that address the Executive Branch's national security concerns relevant to those portions of the application. The Executive Branch's recommendation, consistent with the Cable Landing License Act of 1921,[2] maintains the United States' rights and interests, including promoting U.S. security interests.[3] The Executive Branch's recommendation reflects an assessment that submarine cables are a fundamental element of global communications critical infrastructure, carrying most of the world's internet, voice, and data traffic between continents. As such, it is therefore not in the national security or law enforcement interest of the United States to approve the commercial operation of cables that land

[1] The interested Executive Branch agencies for purposes of this recommendation include the Committee Members and Committee Advisors in Executive Order 13913. *See* Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, 85 Fed. Reg. 19643, 19643-44 ¶ 3 (Apr. 4, 2020).

[2] 47 U.S.C. §§ 34-39.

[3] *See id.* § 35.

directly in Chinese territory, where the government of the People's Republic of China (PRC) has demonstrated the intent to acquire U.S. persons' data to harm U.S. national security. If approved, PLCN's Hong Kong landing station would expose U.S. communications traffic to such collection. This recommendation is based on:

(1) The current national security environment, including new concerns about the PRC's intent to steal or acquire millions of U.S. persons' sensitive personal data, PRC access to foreign data through both digital infrastructure investments and new PRC intelligence and cybersecurity laws, and changes in the market that have transformed subsea cable infrastructure into increasingly data-rich environments that are vulnerable to exploitation;

(2) Concerns about PLCN's PRC-based owners, Dr. Peng Group and Pacific Light Data, including Dr. Peng's support for PRC intelligence and security services under PRC law, questions about Dr. Peng's past compliance with U.S. laws when acquiring U.S. telecommunications assets, and Pacific Light Data's connections to PRC state-owned carrier China Unicom; and

(3) Concerns about the PRC government's recent actions eroding Hong Kong's autonomy through the proposed expansion and applicability of the PRC's national security laws to Hong Kong while at the same time allowing PLCN to further strengthen Hong Kong's status as a hub for international communications critical infrastructure, where a growing share of U.S. communications traffic to the Asia-Pacific must first land on Chinese territory and traverse Chinese-owned or -controlled infrastructure before ultimately reaching final destinations in other parts of Asia.

II. Legal Authority

The President's authority to grant, withhold, revoke, or condition cable landing licenses derives from the Cable Landing License Act of 1921.[4] Executive Order No. 10530 delegates the President's authority to grant licenses to the Commission.[5] The Executive Order requires the Commission to obtain approval from the Secretary of State and to seek advice from any Executive Branch agency the Commission deems necessary before granting or revoking any such license.[6] By regulation, the Commission may act upon a cable landing license only "after obtaining the approval of the Secretary of State and such assistance from any executive department or establishment of the Government as it may require."[7]

Section 2 of the Cable Landing License Act[8] provides the President with the discretion to withhold, revoke, or condition cable landing licenses if the President determines "after due notice and hearing that such action[s] will assist in securing rights for the landing or operation of cables in foreign countries, or in maintaining the rights or interests of the United States or of its citizens in foreign countries, or will promote the security of the United States[.]"[9] The Act also

---

[4] 47 U.S.C. §§ 34-39.

[5] Exec. Order No. 10530 § 5(a), 19 Fed. Reg. 2709 (May 10, 1954). *See also Rules and Policies on Foreign Participation in the U.S. Telecommunications Mkt.*, Report and Order and Order on Reconsideration, 12 FCC Rcd 23891, 23922, ¶ 87 (1997) (hereinafter *1997 Foreign Participation Order*).

[6] Exec. Order No. 10530 § 5(a). *See also 1997 Foreign Participation Order,* 12 FCC Rcd at 23922, ¶ 87.

[7] 47 C.F.R. § 1.767(b) (2019).

[8] 47 U.S.C. § 35.

[9] 47 U.S.C. § 35. S*ee also 1997 Foreign Participation Order,* 12 FCC Rcd at 23946 n.252 (47 U.S.C. § 35 "gives [the Commission] discretion to deny an application if to do so would . . . promote the security of the United States'"); *Telefonica Larga Distancia de Puerto Rico, Inc.,* Memorandum Opinion and Order, 12 FCC Rcd. 5173, 5181-82, ¶¶ 23-25 (1997) (hereinafter *Telefonica Puerto Rico*) (denying a cable landing license application after the State Department,

provides the President with the discretion to grant cable landing licenses conditioned on appropriate mitigation terms.[10]

The Commission has set forth procedures for seeking any advice it deems required from the Executive Branch agencies regarding submarine cable landing license applications.[11] National security and law enforcement concerns have long been treated as important public interest factors in the advice that the Commission seeks from the Executive Branch.[12] The Commission will "accord deference to the expertise of Executive Branch agencies in identifying and interpreting issues of concern related to national security, law enforcement, and foreign policy[.]"[13] Such advice from the Executive Branch "must occur only after appropriate

---

in coordination with DoD, NTIA, and USTR, sent a letter to the Commission stating that the license application should be denied, on the basis that denial would assist in maintaining the rights of U.S. corporations in a foreign country).

[10] *See* 47 U.S.C. § 35 (President "may grant such license upon such terms as shall be necessary to assure just and reasonable rates and service in the operation and use of cables so licensed").

[11] *1997 Foreign Participation Order,* 12 FCC Rcd at 23946, ¶ 130 (noting that the Commission will "continue to consider, . . . other factors consistent with our discretion under the Submarine Cable Landing License Act that may weigh in favor of or against grant of a license"). *See also id.* n. 252 (noting that the Commission's analysis under Section 2 of that Act includes "discretion to deny an application if to do so would . . . 'promote the security of the United States'").

[12] *Id*. at 23919-20, ¶¶ 62-63.

[13] Id. at 23920, ¶ 63. See also *Reform of Rules and Policies on Foreign Carrier Entry into the U.S. Telecommunications Market*, Report and Order, 29 FCC Rcd 4256, 4258, ¶ 4 (2014) (hereinafter 2014 Foreign Carrier Entry Order) ("The Commission's presumption, however, is limited to competition issues; it does not apply to questions regarding national security, law enforcement, foreign policy or trade policy concerns, and such questions are resolved in the same manner regardless of the WTO status of the carrier's home country. The Commission accords deference to Executive Branch agencies in identifying and interpreting issues of concern related to these matters."); *Telefonica Puerto Rico*, 12 FCC Rcd. at 5182-85 ¶¶ 24-33 (adopting the State Department's disapproval of a proposed cable application, in coordination with the advice of DoD, NTIA, and USTR, and noting State Department's determination that "grant of the applications would be inconsistent with the rights and interests of U.S. companies that desire to compete in the Spanish telecommunications market").

coordination among Executive Branch agencies, must be communicated in writing, and will be part of the public file in the relevant proceeding."[14]

The Cable Landing License Act provides the President with broad authority to regulate cable landing licenses.[15] The President may withhold or revoke licenses in order to secure reciprocal cable landing and operation rights in foreign countries, or to maintain the rights of the United States or of its citizens in foreign countries, or to promote the security of the United States.[16] FCC regulations also broadly interpret the Commission's delegated authority. The Commission has expressly declined to limit its review of cable landing license applications to the U.S. landing party and U.S. landing station, and has required all entities with a five percent or greater interest in a cable system and that use U.S. points of the cable system to receive a license before landing or operating a cable.[17] The Commission has noted that management decisions for cables are often made through committees of owners, and that consideration of a foreign or domestic firm's influence on operations "falls squarely within the ambit of the Cable Landing License Act, which requires a license to 'land *or operate*' a submarine cable."[18]

---

[14] *1997 Foreign Participation Order*, 12 FCC Rcd at 23921, ¶ 66. *See also id.* at n.121 ("To the extent the Executive Branch must share classified information with Commission staff, such information is not subject to public disclosure.").

[15] 47 U.S.C. § 35.

[16] *See id.*

[17] 47 C.F.R. § 1.767(h)(2). *See also Review of Commission Consideration of Applications under the Cable Landing License Act*, Report and Order, 16 FCC Rcd 22167, 22196-97, ¶ 57 (2001) (hereinafter *2001 Cable Landing Order*) (declining to limit applicants to landing parties); *Review of Commission Consideration of Applications under the Cable Landing License Act*, Notice of Proposed Rulemaking,15 FCC Rcd 20789, 20824, ¶ 82 (2000) ("We note that the greater a firm's investment in a cable system, the greater ability the firm has to influence the way in which a cable is operated.").

[18] *2001 Cable Landing Order*, 16 FCC Rcd at 22197, ¶ 57 (emphasis in the original).

III. The Pacific Light Cable Network Cable System

Applicants Pacific Light Data Communication Co. Ltd. (Pacific Light Data), GU Holdings Inc. (Google),[19] and Edge Cable Holdings USA, LLC (Facebook)[20] (collectively, the Applicants) seek a license to land and operate the PLCN fiber optic submarine cable system. PLCN will extend between the United States, Hong Kong, Taiwan, and the Philippines.[21]

PLCN would be the first subsea cable directly connecting the United States and Hong Kong.[22] At 144 terabits per second (Tbps), PLCN has the largest design capacity of any existing or announced cable system on the U.S.-Asia route.[23] The Applicants state that PLCN would lower costs for bandwidth to Asia by increasing competition.[24] The Applicants propose to use PLCN capacity to connect their affiliates' data centers in the United States and Asia.[25] The Applicants further state that PLCN would interconnect with other subsea and terrestrial cables and enhance the dynamic routing capabilities of carriers and service providers in the region.[26]

---

[19] GU Holdings Inc. is a subsidiary of Google LLC. Exhibit 1 at EB-PUBLIC-3, *Streamlined Submarine Cable Landing License Applications, Accepted for Filing,* Public Notice, Report No. SCL-00204S at 3 (Nov. 1, 2017) (hereinafter *PLCN Public Notice*).

[20] *See id.* (Edge Cable Holdings USA, LLC is a subsidiary of Facebook, Inc.).

[21] *Id.* at EB-PUBLIC-2, *PLCN Public Notice* at 2.

[22] Exhibit 100 at EB-PUBLIC-1733, Amendment to Application for a Cable Landing License, Appendix D at 1, SCL-AMD-20171227-00025 (Dec. 27, 2017) (hereinafter *PLCN Application Amendment*).

[23] Exhibit 2 at EB-PUBLIC-8, *Application for a Cable Landing License, Streamlined Processing* Requested, at 4 SCL-LIC-20170421-00012 (filed Apr. 21, 2017) (hereinafter *PLCN Application*). *See also* Exhibit 3 at EB-PUBLIC-48, *PLCN Project*, Dr. Peng Group, https://www.drpeng.com.cn/en/business/overseas/plcn (last visited Mar. 21, 2020).

[24] Exhibit 2 at EB-PUBLIC-8, *PLCN Application* at 4.

[25] Exhibit 2 at EB-PUBLIC-7, *PLCN Application* at 3. *See also* Exhibit 3 at EB-PUBLIC-48.

[26] Exhibit 2 at EB-PUBLIC-9, *PLCN Application* at 5.

PLCN map with United States, Taiwan, Philippines, and Hong Kong cable landing sites[27]

Examples of such potential regional interconnections follow. After PLCN was announced as the first direct U.S.-Hong Kong cable, two separate consortiums filed applications with the FCC in 2018 for two separate cable systems on the same route.[28] These two cable systems, Hong Kong-Americas (HKA) and Bay to Bay Express (BtoBE), are financed in part by the PRC government through state-owned carriers and include major U.S. information and communications technology (ICT) service providers as co-owners.[29] In 2019, an application for the Hong Kong-

[27] Exhibit 4 at EB-PUBLIC-50, TeleGeography, *Pacific Light Cable Network - PLCN*, Submarine Cable Map, https://www.submarinecablemap.com/#/submarine-cable/pacific-light-cable-network-plcn (last visited Mar. 21, 2020) (annotated and modified to show landing sites). *See also* Exhibit 2 at EB-PUBLIC-19, *PLCN Application* at Appendix A (Geographical Overview).

[28] Exhibit 5 at EB-PUBLIC-51, Streamlined Submarine Cable Landing License Applications, Accepted for Filing, Public Notice, Report No. SCL-00232S (Dec. 26, 2018) (hereinafter BtoBE Public Notice); Exhibit 6 at EB-PUBLIC-54, Streamlined Submarine Cable Landing License Applications, Accepted for Filing, Public Notice, Report No. SCL-00223S (Aug. 23, 2018) (hereinafter HKA Public Notice).

[29] The HKA cable owners include Facebook (Edge Cable Holdings USA, LLC), China Telecom (China Telecommunications Corporation and subsidiary China Telecom Global), and China Unicom (China United Network Communications Group Company Limited). *See* Exhibit 6 at EB-PUBLIC-55, *HKA Public Notice*. The BtoBE cable owners include Facebook (Edge Cable Holdings USA, LLC), China Mobile (China Mobile International Limited), and Vadata, Inc. (a

Guam (HK-G) cable system, another U.S.-Hong Kong cable connection, was filed with the FCC.[30]

PLCN's main trunk consists of six fiber pairs extending between California and Hong Kong.

- Hong Kong-based Pacific Light Data owns and controls four of six fiber pairs on the main trunk and has 66.67 percent voting and participation rights on the main trunk.[31]
- Google owns and controls one of the six fiber pairs on the main trunk and has 16.67 percent voting and participation rights on the main trunk.[32]
- Facebook owns and controls one of the six fiber pairs on the main trunk and has 16.67 percent voting and participation rights on the main trunk.[33]

Pacific Light Data would serve as the Hong Kong landing party and Google would serve as the U.S. landing party for PLCN.[34] In Hong Kong, the PLCN cable would first land at a facility in Deep Water Bay, Hong Kong, which is owned by PCCW Global (HK), Ltd., a local Hong Kong carrier.[35] [redacted]

subsidiary of Amzaon.com, Inc.). *See* Exhibit 5 at EB-PUBLIC-53, *BtoBE Public Notice*.

[30] Exhibit 102 at EB-PUBLIC-1780, *Streamlined Submarine Cable Landing License Applications, Accepted for Filing,* Public Notice, Report No. SCL-00256S (Dec. 27, 2019) (hereinafter *HK-G Public Notice*).

[31] Exhibit 1 at EB-PUBLIC-2, -14, *PLCN Public Notice* at 2, 10; *see also* Exhibit 1002 at CONF-PLCN-ALL-32, May 2019 Responses to Triage Questions received from all PLCN Applicants, Appendix 2 (System Ownership) (originally produced as PLCN-000387).

[32] Id.

[33] Id.

[34] Exhibit 1 at EB-PUBLIC-2, *PLCN Public Notice* at 2.

[35] Exhibit 103 at EB-PUBLIC-1786, *Third Supplement to Application for a Cable Landing License (Streamlined Processing Requested)*, SCL-LIC-20170421-00012 (hereinafter *PLCN*

In addition to its minority ownership in the U.S.-Hong Kong main trunk, Google (through an affiliate) owns 100 percent of the PLCN segment that branches off the main trunk to Taiwan.[38] From Taiwan, Google's fiber pair returns to the main trunk and proceeds to the Deep Water Bay facility in Hong Kong, connecting the United States and Hong Kong with an intermediate stop in Taiwan.[39] Likewise, Facebook (through an affiliate) owns 100 percent of the two PLCN segments that branch off the main trunk to the Philippines (San Fernando and Baler).[40] From the Philippines, Facebook's fiber pair returns to the main trunk and proceeds to the Deep Water Bay facility in Hong Kong, connecting the United States and Hong Kong with two intermediate stops in the Philippines.[41]

Application Third Supplement); Exhibit 1002 at CONF-PLCN-ALL-33 to -34, May 2019 Responses to Triage Questions received from all PLCN Applicants, Appendix 2 (System Ownership) (originally produced as PLCN-000388 to -389) (hereinafter *PLCN Applicants' May 2019 Triage Responses*).

[36] *Id.* at CONF-PLCN-ALL-31 to -34 (originally produced as PLCN-000386 to -389).

[37] Id.

[38] Exhibit 1 at EB-PUBLIC-2, *PLCN Public Notice* at 2; Exhibit 1002 at CONF-PLCN-ALL-31 to -34, *PLCN Applicants' May 2019 Triage Responses*, Appendix 2 (System Ownership) (originally produced as PLCN-000386 to -389).

[39] Exhibit 1 at EB-PUBLIC-2, *PLCN Public Notice* at 2.

[40] Id.

[41] Id.

Google and Facebook have stated that their respective fiber pairs connecting the United States, Philippines, and Taiwan can operate independently of any Hong Kong connection, as well as independently of the four fiber pairs owned by Pacific Light Data.[43]

IV. The current national security landscape has raised new concerns

The current national security landscape raises new concerns, which have emerged and evolved over the last decade. In September 2015, the United States and China issued a historic

[42] Derived from Exhibit 1002 at CONF-PLCN-ALL-31 to -34, *PLCN Applicants' May 2019 Triage Responses*, Appendix 2 (System Ownership) (originally produced as PLCN-000386 to -389); Exhibit 103 at EB-PUBLIC-1786, *PLCN Application Third Supplement* at 4; Exhibit 1 at EB-PUBLIC-2, *PLCN Public Notice* at 2.

[43] Exhibit 104 at EB-PUBLIC-1800, *Request for Special Temporary Authority,* SCL-STA-20200129-00006 at 5 (filed Jan. 29, 2020) (hereinafter *PLCN Commercial Operations STA*).

bilateral cyber declaration, when the leaders of both countries publicly committed that governments should not conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets and other confidential business information, with the intent of providing competitive advantage to companies or commercial sectors.[44] China also made similar cyber commitments to the international community at the G20 Summit that year.[45] In January 2017, the Commission granted a license application for a cable system connecting the United States to China, the New Cross Pacific (NCP) cable system.[46] As described below, however, several events have come to light that indicate the PRC's intent and capability to collect U.S.

[44] Exhibit 9 at EB-PUBLIC-67 to -68, *Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference*, White House (Sept. 25, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.; Exhibit 10 at EB-PUBLIC-87 to -88, *Fact Sheet: President Xi Jinping's State Visit to the United States,* White House (Sept. 25, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

[45] Exhibit 11 at EB-PUBLIC-95, *G20 Leaders' Communiqué, Antalya Summit, 15-16 November 2015,* G20 (Nov. 16, 2015), https://www.consilium.europa.eu/media/23729/g20-antalya-leaders-summit-communique.pdf.

[46] In 2015, the Commission received the application for the New Cross Pacific (NCP) cable system connecting the United States, China, Japan, Taiwan, and the Republic of Korea. *See Streamlined Submarine Cable Landing License Applications Accepted for Filing,* Public Notice, Report No. SCL-00170S (Dec. 3, 2015) (identifying application filed by Microsoft (through affiliates Microsoft Infrastructure Group, LLC and Microsoft Operations Pte Ltd), China Mobile (China Mobile International Limited), China Telecom (China Telecommunications Corporation, China Unicom (China United Network Communications Group Company Limited), and other regional carriers. The NCP license was granted subject to conditions on January 12, 2017. *See* Exhibit 7 at EB-PUBLIC-58, *Actions Taken Under Cable Landing License Act,* Public Notice, Report No. SCL-00193 (Jan. 13, 2017) (hereinafter *NCP Grant Public Notice*).

persons' data to harm U.S. national security. Together, these events make the context of the current national security landscape different and concerning.

By 2018, the U.S. government made public allegations that the PRC had failed to live up to its obligations under the 2015 declaration. First, in November 2017, the Department made public that China had failed to respond meaningfully to a request for cooperation in the investigation of employees at a purported internet security firm that had stolen trade secrets and other commercial information.[47] Then, in December 2018, DOJ announced the indictment of two hackers associated with a PRC intelligence service for their alleged hacking of managed service provider (MSP) networks.[48] The Chinese hackers allegedly sought, among other data, intellectual property and confidential information of MSP clients in at least 12 countries, including leading U.S. companies in the banking and finance, telecommunications and consumer electronics, medical equipment, healthcare, and other sectors.[49] The Executive Branch made

[47] Exhibit 119 at EB-PUBLIC-2114, *U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage*, U.S. Dep't of Justice (Nov. 27, 2017), https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations. *See also* Exhibit 120 at EB-PUBLIC-2122, Chris Bing, *DOJ reveals indictment against Chinese cyberspies that stole U.S. business secrets*, CyberScoop (Nov. 27, 2017), https://www.cyberscoop.com/boyusec-china-doj-indictment/ (quoting DOJ statement that the Department received "no meaningful response" when it requested PRC government's assistance in investigating and putting a stop to indicted Chinese hackers).

[48] Exhibit 13 at EB-PUBLIC-104, Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information, U.S. Dep't of Justice (Dec. 20, 2018), https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

[49] *Id.* *See also* Exhibit 16 at EB-PUBLIC-113, *United States v. Zhu Hua et al.*, No. 18-cr-891, Indictment (S.D.N.Y. filed Dec. 17, 2018).

clear that the activity alleged in the indictment was intended to advantage Chinese companies and violated the declaration that China had made in 2015.[50]

A. The U.S. government has raised new concerns about the PRC's acquisitions of millions of Americans' sensitive personal data through both illegal and legitimate means

1. Chinese state- and non-state cyber actors have acquired sensitive personal data pertaining to millions of Americans by breaching the networks of Equifax, Anthem, and OPM

In February 2020, DOJ announced an indictment of Chinese military hackers for their alleged role in the 2017 Equifax data breach, calling the scale of the Chinese government's data theft "staggering."[51] The Equifax indictment charged four members of the Chinese People's Liberation Army (PLA) with hacking into the computer systems of credit-reporting agency Equifax and thereby stealing the sensitive personal information of 145 million Americans—nearly half of all American citizens.[52]

---

[50] Exhibit 12 at EB-PUBLIC-102, *Deputy Attorney General Rod J. Rosenstein Announces Charges Against Chinese Hackers*, U.S. Dep't of Justice (Dec. 20, 2018), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-announces-charges-against-chinese-hackers; Exhibit 121 at EB-PUBLIC-2129, @AmbJohnBolton. "Today, @TheJustice Dept indicted hackers who conduct unprecedented intellectual property theft on behalf of the Chinese Ministry of State Security. We stand w/ allies & partners in calling out this shameful violation of the 2015-US-China Cyber Commitments." *Twitter* (Dec. 20, 2018, 10:55 a.m.), https://twitter.com/AmbJohnBolton/status/1075781730831876096.

[51] Exhibit 15 at EB-PUBLIC-111, *Attorney General William P. Barr Announces* Indictment of Four Members of China's Military for Hacking into Equifax, U.S. Dep't of Justice (Feb. 10, 2020) (hereinafter Barr Announcement), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military; Exhibit 17 at EB-PUBLIC-136, United States v. Wu Zhiyong et al., No. 20-cr-046, Indictment (N.D. Georgia filed Jan. 28, 2020); Exhibit 14 at EB-PUBLIC-108, Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax, U.S. Dep't of Justice (Feb. 10, 2020), https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking.

[52] Exhibit 15 at EB-PUBLIC-111, *Barr Announcement*; Exhibit 17 at EB-PUBLIC-137.

According to the Attorney General, the Equifax breach presented a continuing pattern of "China's voracious appetite for the personal data of Americans," including the theft of personnel records from the U.S. Office of Personnel Management (OPM), and the intrusion into the Anthem health insurance company.[53]

In May 2019, DOJ announced the indictments of Chinese cyber actors for their alleged role in the 2015 Anthem data breach, which resulted in the loss of sensitive personal information of more than 78 million people from Anthem's computer network.[54]

In September 2016, a congressional report on the OPM data breach concluded that foreign cyber actors stole personnel files of 4.2 million current and former federal government employees, security clearance background investigation information on 21.5 million individuals, and the fingerprint data of 5.6 million individuals.[55] According to the House of Representatives report, the "*intelligence and counterintelligence value of the stolen background information for a foreign state cannot be overstated*[.]"[56] In September 2018, then-National Security Advisor John Bolton specifically attributed the OPM data breach to China,[57] illuminating the concerns raised

---

[53] Exhibit 15 at EB-PUBLIC-111, *Barr Announcement*.

[54] Exhibit 18 at EB-PUBLIC-160, Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People, U.S. Dep't of Justice (May 9, 2019), https://www.justice.gov/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including; Exhibit 19 at EB-PUBLIC-163, United States v. Fujie Wang et al., No. 19-cr-153, Indictment (S.D. Ind. filed May 7, 2019).

[55] Exhibit 20 at EB-PUBLIC-180, Majority Staff Report*, The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, at v, Committee on Oversight and Government Reform, U.S. House of Representatives, 114th Cong. (Sept. 7, 2016), *available at* https://republicans-oversight.house.gov/report/opm-data-breach-government-jeopardized-national-security-generation/.

[56] *Id.* at EB-PUBLIC-185, at vi (emphasis in the original).

[57] Exhibit 122 at EB-PUBLIC-2132, Ian Smith, *Bolton Confirms China Was Behind OPM Data Breaches,* FedSmith (Sept. 21, 2018), https://www.fedsmith.com/2018/09/21/bolton-confirms-

in the 2016 House report

Each data theft is troubling on its own. But the probability that PRC intelligence services have gained access to the sensitive personal data of millions of U.S. persons raises significant national security concerns. In announcing the Equifax indictment, the Attorney General noted that the stolen data not only had economic value, but could also "feed China's development of artificial intelligence tools as well as the creation of intelligence targeting packages."[58] The U.S. intelligence community has previously warned of the capabilities that a foreign adversary may gain with access to large volumes of U.S. persons' data. In July 2015, then-director of the National Security Agency Admiral Michael Rogers stated that "we need to recognize that increasingly data has a value all its own[.]"[59] He noted that, with big data analytics, a foreign adversary could gain intelligence insights useful for targeting U.S. persons; for example, the foreign adversary might know whether a U.S. person traveling to a foreign country was just a tourist or had other reasons for travel.[60] These concerns provide additional background for the Executive Branch's concerns, as a submarine cable like PLCN landing in Hong Kong would provide additional opportunities for PRC authorities to collect U.S. communications traffic for further big data analysis. By combining personnel data with travel records, health records, and

china-behind-opm-data-breaches/.

[58] Exhibit 15 at EB-PUBLIC-111.

[59] Exhibit 115 at EB-PUBLIC-2018, *Beyond the Build: Leveraging the Cyber Mission Force,* Aspen Institute (July 23, 2015) (Transcript of statement by Adm. M. Rogers), http://aspensecurityforum.org/wp-content/uploads/2015/07/Beyond-the-Build-Leveraging-the-Cyber-Mission-Force.pdf.

[60] *Id.* at EB-PUBLIC-2018 to -19.

credit information, PRC intelligence services may have the capability to create in just a few years a database more detailed than any nation has ever possessed about one of its rivals.[61]

2. Congress and the President have raised concerns that PRC investments could facilitate access to U.S. companies' sensitive personal data in ways that threaten national security

In August 2018, Congress responded to new concerns that PRC investments could enable access to U.S. companies' sensitive personal data in ways that threaten national security by passing the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA).[62] Senator John Cornyn, FIRRMA's sponsor, stated that he had "major concerns regarding U.S. data, especially the personally identifiable information (PII) of U.S. citizens . . . The Chinese Communist Party considers data to be a national strategic resource . . . when U.S. companies are forced to on-shore data into China, it can have major U.S. national security implications."[63] In FIRRMA, Congress urged the Committee on Foreign Investment in the United States (CFIUS) to review investments that are likely to expose "personally identifiable information, genetic

[61] *See, e.g.,* Exhibit 22 at EB-PUBLIC-428, Garrett M. Graff, *China's Hacking Spree Will Have a Decades-Long Fallout*, Wired (Feb. 11, 2020), https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/; Exhibit 23 at EB-PUBLIC-432, Ben Kochman, *Equifax Hack Shows China's Expanding Hunger for Data*, Law360 (Feb. 11, 2020), https://www.law360.com/cybersecurity-privacy/articles/1242594/equifax-hack-shows-china-s-expanding-hunger-for-data ("China is building a digital dossier on individual American citizens. [ ] And through this one [Equifax] breach alone, they built half of that dossier."). *See also* Exhibit 21 at EB-PUBLIC-422, David Sanger, *Marriott Concedes 5 Million Passport Numbers lost to Hackers Were Not Encrypted,* New York Times (Jan. 4, 2019), https://www.nytimes.com/2019/01/04/us/politics/marriott-hack-passports.html.

[62] Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), Pub. L. No. 115-232, §§ 1702-1728, 132 Stat. 2174-2207 (2018).

[63] Exhibit 24 at EB-PUBLIC-439-40, CFIUS Reform: Examining the Essential Elements: Hearing on S. 2098 Before the S. Comm. on Banking, Hous., and Urban Affairs, 115th Cong. 6–7 (2018) (statement of Sen. John Cornyn).

information, or other sensitive data of United States citizens to access by a foreign government or foreign person that may exploit that information in a manner that threatens national security."[64] FIRRMA provided CFIUS with express authority to review non-controlling foreign investments in a U.S. business that "maintains or collects sensitive personal data of United States citizens that may be exploited in a manner that threatens national security."[65]

In February 2020, the U.S. Department of the Treasury adopted new CFIUS regulations implementing Congress's directives in FIRRMA.[66] The regulations addressed concerns that some businesses may collect personal data from sensitive populations, such as federal government employees or contractors, either by targeting these populations or by collecting information on such a large scale that data from these groups would likely be included.[67] Foreign access to certain types of financial data also raised national security concerns if the data could be used to target individuals vulnerable due to financial hardship.[68] Likewise, foreign access to collections of personal insurance information, health-related data, nonpublic electronic communications, geolocation data, biometric identification data, government identification or

---

[64] FIRRMA, Pub. L. No. 115-232, § 1702(c)(5), 132 Stat. 2176-77.

[65] *Id.* § 1703(a)(4)(B)(iii)(III), 132 Stat. 2178.

[66] *Provisions Pertaining to Certain Investments in the United States by Foreign Persons*, 85 Fed. Reg. 3112 (Jan. 17, 2020) (final rule effective Feb. 13, 2020) (hereinafter CFIUS Final Rule). See also *Provisions Pertaining to Certain Investments in the United States by Foreign Persons*, 84 Fed. Reg. 50174 (Sept. 24, 2019) (proposed rule) (hereinafter CFIUS Proposed Rule).

[67] *See CFIUS Final Rule*; 85 Fed. Reg. at 3118-19, 3132-33 (responding to comments on the proposed definitions for sensitive personal data and providing adopted definitions in section 800.241); *CFIUS Proposed Rule*, 84 Fed. Reg. at 50177-78 (explaining proposed definitions for sensitive personal data in Section 800.241).

[68] *See CFIUS Final Rule*, 85 Fed. Reg. at 3132-33 (final definition of sensitive personal data); *CFIUS Proposed Rule*, 84 Fed. Reg. at 50178.

security clearance information, and genetic information could also threaten national security.[69] Notably, parties to certain types of transactions involving a substantial ownership by a foreign government in the foreign investor must file with CFIUS if the U.S. business subject to the transaction maintains or collects this sensitive personal data.[70]

In March 2020, the President issued an Executive Order prohibiting the acquisition of a U.S. corporation by a Chinese public company, and prohibiting the proposed acquirer from accessing any U.S. customer data and hotel guest data.[71] The President found that there was credible evidence that the Chinese public company and its Hong Kong subsidiary, through acquiring an interest in a U.S. corporation, "might take action that threatens to impair the national security of the United States."[72] The President prohibited the acquisition, and ordered the Chinese purchaser to "divest all interests in . . . data (including customer data managed and stored by [the target U.S. corporation])."[73] The President also ordered the Chinese purchaser to "refrain from accessing . . . hotel guest data through [the target U.S. corporation]" and to "ensure that controls are in place to prevent any such data access until such time as the divestment has been completed[.]"[74]

---

[69] *See CFIUS Final* Rule, 85 Fed. Reg. at 3132.

[70] *Id.* at 3140 (defining types of transactions subject to mandatory declarations).

[71] Executive Order Regarding the Acquisition of StayNTouch, Inc. by Beijing Shiji Information Technology Co., Ltd., 85 Fed. Reg. 13719 (Mar. 10, 2020).

[72] Id.

[73] Id.

[74] *Id.* at 13719-20.

B. New concerns about the data that the PRC government could access through infrastructure investments and new cybersecurity and intelligence laws

1. Digital infrastructure projects through the PRC One Belt, One Road (OBOR) initiative support PRC ambitions of becoming a "digital superpower"

In December 2017, the White House National Security Strategy warned that "China's infrastructure investments . . . reinforce its geopolitical aspirations" and that China sought to displace the United States in the Indo-Pacific region.[75] Since 2013, the PRC government has made massive infrastructure investments through the One Belt, One Road (OBOR) initiative.[76] Although focused on traditional physical infrastructure projects ostensibly directed towards economic goals, the OBOR initiative has more recently pivoted to cyberspace through the Digital Silk Road initiative.[77] The OBOR and Digital Silk Road initiatives are aimed at connecting the world through a web of PRC-funded infrastructure.[78] Digital infrastructure investments have become increasingly important for the PRC's goal of turning China into a "cyber superpower,"[79]

---

[75] Exhibit 26 at EB-PUBLIC-535, *National Security Strategy of the United States of America,* at 46 White House (Dec. 2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf. *See also id.* at EB-PUBLIC-511 ("The United States will expand our focus beyond protecting networks to protecting the data on those networks so that it remains secure—both at rest and in transit.").

[76] Exhibit 27 at EB-PUBLIC-559 to -566, 2018 Report to Congress of the U.S.-China Economic and Security Review Commission, at 259 115th Cong.(2018) (Chapter 3, Section 1: Belt and Road Initiative and Digital Silk Road), https://www.uscc.gov/sites/default/files/2019-09/2018%20Annual%20Report%20to%20Congress.pdf.

[77] *Id.* at EB-PUBLIC-564.

[78] *Id.* at EB-PUBLIC-559; Exhibit 28 at EB-PUBLIC-605, D. Kliman and A. Grace, *Power Play: Addressing China's Belt and Road Strategy*, Center for a New American Security 1 (Sept. 2018) (Executive Summary), https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-Power-Play-Addressing-Chinas-Belt-and-Road-Strategy.pdf?mtime=20180920093003. *See also* Exhibit 29 at EB-PUBLIC-664 to -665, *Assessment on U.S. Defense Implications of China's Expanding Global Access,* U.S. Dep't of Defense 12 (Dec. 2018).

[79] Exhibit 30 at EB-PUBLIC-682, DigiChina, *Translation: Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference,* New America (last visited Mar. 9, 2020), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-

as controlling the flow of data becomes increasingly important for shifting the balance of geopolitical power in China's favor.[80] While such investments alone would not cause concern, the combination of this objective with the state-sponsored theft of U.S. persons' data and targeted acquisitions of U.S. companies with sensitive personal data earlier described paints a different, more troubling picture.

With the encouragement of state policy, Chinese enterprises have significantly increased investments in ICT infrastructure. Such investments have focused on data centers, data storage infrastructure, and land and subsea fiber optic cables.[81] Between 2012 and 2015, Chinese companies were involved with only seven percent of disclosed global submarine cable projects, and exclusively with projects that connected either to the Chinese mainland, Taiwan, or Hong Kong.[82] In contrast, between 2016 and 2019, Chinese companies are estimated to have participated in 20 percent of all cable construction projects, more than half of which took place outside the South China Sea.[83]

In November 2018, the U.S. China Economic and Security Review Commission warned that as "Chinese companies lay fiber optic cable, [ ] they are expanding China's influence over

---

jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/. *See also* Exhibit 28 at EB-PUBLIC-614 ("The Belt and Road [another translation of One Belt, One Road] is advancing Beijing's intention to become the world's leading information technology power.").

[80] Exhibit 32 at EB-PUBLIC-708, Andrew Kitson and Kenny Liew, *China Doubles Down on Its Digital Silk Road,* Center for Strategic and International Studies (Nov. 14, 2019), https://reconnectingasia.csis.org/analysis/entries/china-doubles-down-its-digital-silk-road/.

[81] *Id.* at EB-PUBLIC-708 to -709.

[82] Exhibit 33 at EB-PUBLIC-720, Stacia Lee, *The Cybersecurity Implications of Chinese Undersea Cable Investment,* Univ. of Washington Jackson School of Int'l Studies (Feb. 6, 2017), https://jsis.washington.edu/eacenter/2017/02/06/cybersecurity-implications-chinese-undersea-cable-investment/.

[83] Id.

the global digital economy to align more closely with Beijing's vision of internet governance."[84] DOD has raised similar concerns, noting that the PRC has linked the OBOR initiative to building ICT infrastructure and to promoting China's goals for cybersecurity and global internet governance reform.[85] Silicon Valley has also taken note. In October 2019, Facebook's founder, Mark Zuckerberg, stated his concerns "about the future of the global internet. China is building its own internet focused on very different values, and is now exporting their vision of the internet to other countries."[86]

The China Academy of Information and Communications Technology (CAICT), an influential government think tank underneath the PRC Ministry of Industry and Information Technology (MIIT), has provided more details on China's subsea cable policy.[87] CAICT has openly urged Chinese enterprises to "actively participate in the global laying of submarine optical cables and actively promote the inception and development of related industries."[88]

---

[84] Exhibit 27 at EB-PUBLIC-564.

[85] Exhibit 29 at EB-PUBLIC-665.

[86] Exhibit 34 at EB-PUBLIC-736, Mark Zuckerberg, *Standing for Voice and Free Expression*, Facebook.com (Oct. 17, 2019), https://www.facebook.com/notes/mark-zuckerberg/standing-for-voice-and-free-expression/10157267502546634/.

[87] *See* Exhibit 36 at EB-PUBLIC-749, *White Paper on China International Optical Cable Interconnection*, China Academy of Information and Communications Technology (Aug. 2018), http://www.caict.ac.cn/english/research/whitepapers/202003/P020200327550620516330.pdf. The PRC Ministry of Industry and Information Technology (MIIIT) has significant responsibility for managing China's digital strategy and regulating ICT sector industrial policy. *See* Exhibit 35 at EB-PUBLIC-741, Paul Triolo, Samm Sacks, Graham Webster, Rogier Creemers, China's Cybersecurity Law One Year On, New America (Nov. 30, 2017), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/. CAICT has been an important interlocutor for foreign ICT firms regarding policies and standards development. *Id.*

[88] Exhibit 36 at EB-PUBLIC-751 (Foreword). The paper also notes that the "Information and Communication Infrastructure Interconnection is an Important Cooperative Content" of the OBOR initiative (referred to as Belt and Road Initiative, or BRI). *Id.* at EB-PUBLIC-770.

CAICT stated that the "[d]evelopment [t]rends of [c]ollaboration [b]etween [s]ubmarine [c]ables and [d]ata [c]enters is [o]bvious," and that the "submarine cable provides information transmission channels, and data centers store and process information. To this end, the development path of the information hub is increasingly clear."[89]

The PRC's influence in cyberspace is rapidly growing due to Chinese companies' ownership and provision of the physical infrastructure underlying cyberspace.[90] The Internet is commonly misconceived as an intangible and virtual abstraction, but at its most fundamental

---

[89] *Id.* at EB-PUBLIC-758, 760. CAICT also noted that "Internet giants such as Google, Microsoft, and Facebook are becoming the leading force in constructing international submarine cables[,]" and that "[d]ata center interconnect (DCI) has become an important goal for Internet giants in their participation in international submarine cable construction." *Id.* at EB-PUBLIC-758 to -759.

[90] Exhibit 37 at EB-PUBLIC-785, Julia Voo, *A Case for Fortifying the BUILD Act: The U.S., China, and Internet Infrastructure in the Global South*, Belfer Center, Harvard Kennedy School (July 2019), https://www.belfercenter.org/publication/case-fortifying-build-act-us-china-and-internet-infrastructure-global-south; *see also* Exhibit 38 at EB-PUBLIC-800, John Hemmings and Patrick Cha, *Exploring China's Orwellian Digital Silk Road,* The National Interest (Jan. 7, 2020), https://nationalinterest.org/feature/exploring-china%E2%80%99s-orwellian-digital-silk-road-111731 ("By acting as network architects and administrators, Beijing will be privy to data streams in real-time across a large portion of the world, enabling them to develop influence and power across a number of different matrixes."). *See also* Exhibit 33 at EB-PUBLIC-722 to -723 ("While Chinese investment may prove affordable and attractive, history dictates that reliance upon Chinese infrastructure can have deleterious and politically-motivated cybersecurity consequences – one need only consider the case of Vietnam, where Chinese investors have dominated both physical and digital infrastructure development. When Vietnam expressed its disapproval of China's position on the South China Sea,. . . Chinese hackers [ ] exploited their knowledge of Vietnam's airport systems – which were provided by the Chinese – to hack and suspend airport computers as well as airline websites."); *see also* Exhibit 31 at EB-PUBLIC-689, -700, Eric Rosenbach and Katherine Mansted, *The Geopolitics of Information,* Belfer Center, Harvard Kennedy School (May 28, 2019), https://www.belfercenter.org/publication/geopolitics-information ("*Limit foreign ownership and provide resources to support firms in key information sectors*. Over the past decade China has systematically targeted investment in and ownership of firms developing data-driven technologies like AI. Congress has increased limitations and oversight of foreign ownership and involvement in data-rich sectors. While important, this should be supplemented with new incentives to sustain American tech firms whose technology does not have an immediate commercial application.") (emphasis in the original).

level, there is a tangible physical layer[91] consisting of the fiber optic cables, satellites, and networking equipment such as routers and switches.[92] On top of the physical layer are other virtual layers that carry communications at more abstract levels, such as the level in which end users interact with software applications. Although the Internet is designed to be a redundant network, providing many alternate routes in case one goes down, the physical layer is the least redundant.[93] According to a China cyber policy researcher at the Harvard Kennedy School, "China's ownership of the physical infrastructure theoretically means that the Chinese government can control it and access information when needed. This access to significant amounts of data gives China an advantage over the [United States] in intelligence collection. Because of this enhanced intelligence collection, China might gain an economic, political, or security advantage over the [United States]."[94]

---

[91] The Internet is commonly conceptualized as a communications system partitioned into seven abstraction layers, beginning with the least abstract, physical layer (Layer 1, where digital bits are converted into physical—*i.e.,* optical, electrical, or radio—signals) up to highest and most virtual layer (Layer 7, where the end user interacts with the software application). *See* Exhibit 39 at EB-PUBLIC-807, *What is the OSI Model?*, Cloudflare, (last visited Mar. 2, 2020), https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/.

[92] Exhibit 37 at EB-PUBLIC-786.

[93] *Id.* at EB-PUBLIC-788.

[94] *Id.* at EB-PUBLIC-786. *See also* Exhibit 28 at EB-PUBLIC-614 to -615 ("The Belt and Road is advancing Beijing's intention to become the world's leading information technology power."); *see also* Exhibit 40 at EB-PUBLIC-838 to -39, Jonathan E. Hillman, *Influence and Infrastructure: The Strategic Stakes of Foreign Projects,* Center for Strategic and Int'l Studies (Jan. 2019), https://www.csis.org/analysis/influence-and-infrastructure-strategic-stakes-foreign-projects. (comparing the United Kingdom's 19th century dominance of global subsea telegraph cable system through infrastructure ownership and operation with PRC's rising dominance of global subsea fiber optic cable systems).

2. New cybersecurity and intelligence laws provide the PRC government with greater legal access to data entering Chinese territory or on Chinese-owned infrastructure

Since 2017, the PRC government has adopted cybersecurity and intelligence laws and regulations that greatly expand its ability to access any data—including foreign data—entering Chinese territory or traveling through Chinese-owned or -controlled infrastructure outside of China. According to one observer, such laws may perpetuate the "leadership's narrative . . . that the Chinese Communist Party-state is now strong enough to call for intelligence cooperation even from foreigners doing business in China."[95]

The 2017 Cybersecurity Law, and the regulatory regime implementing it, applies to foreign-owned companies in China on the same basis as all Chinese entities, and no information contained on any server within Chinese territory is exempt.[96] Article 28 of the Cybersecurity Law states that "[n]etwork operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law."[97] "Network operators" are broadly defined as "network owners, managers, and network service providers."[98] This vague definition ensnares both foreign and Chinese network operators that own or manage a network or provide

[95] Exhibit 41 at EB-PUBLIC-851, Murray Scot Tanner, *Beijing's New National Intelligence Law: From Defense to Offense,* Lawfare (July 20, 2017), https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.

[96] Exhibit 42 at EB-PUBLIC-855, Steve Dickinson, *China's New Cybersecurity Program: NO Place to Hide,* Harris Bricken (Sept. 30, 2019), https://www.chinalawblog.com/2019/09/chinas-new-cybersecurity-program-no-place-to-hide.html.

[97] Exhibit 43 at EB-PUBLIC-872, Rogier Creemers, Paul Triolo, and Graham Webster, *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)*, New America (June 29, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

[98] *Id.* at EB-PUBLIC-888 (2017 Cybersecurity Law, Article 76(3), providing definition of "network operators").

online services anywhere within China.[99]

In May 2019, the Cyberspace Administration of China (CAC)[100] released "Draft Data Security Management Measures" (DDSMM) to provide further guidance for implementing the 2017 Cybersecurity Law.[101] Article 36 of the DDSMM states that when "the relevant departments of the State Council, in order to fulfill the requirements of their responsibilities in safeguarding national security[. . .] request network operators provide them with relevant data in their possession, network operators should provide it."[102] Network operators collecting "important data or sensitive personal information" are also required to register with local cybersecurity and informatization departments providing "the scale, method, scope, type, retention period, etc., of data collection and use[.]"[103] Network operators that fail to cooperate with the PRC government can expect repercussions such as "suspension of business operations, restructuring of business . . . and/or revocation of relevant business licenses and permits[.]"[104]

The 2017 Intelligence Law provides PRC intelligence services with greater powers to compel Chinese citizens and organizations "to cooperate, assist, and support Chinese intelligence

---

[99] *Id.* at EB-PUBLIC-865 (2017 Cybersecurity Law, Article 2). *See also* Exhibit 44 at EB-PUBLIC-892, *White Paper: Implementing China's Cybersecurity Law,* Jones Day (Aug. 2017), https://www.jonesday.com/en/insights/2017/08/implementing-chinas-cybersecurity-law.

[100] Exhibit 35 at EB-PUBLIC-741 (The CAC is a "relatively new agency seeking to assert its authority over cybersecurity and informatization (*i.e.* digital economy and the ICT industry), [and] draws its authority from its status as the office of a Xi-led Leading Small Group.").

[101] Exhibit 46 at EB-PUBLIC-914, Katharine Tai, Lorand Laskai, Rogier Creemers, Mingli Shi, Kevin Neville, and Paul Triolo, *Translation: China's New Draft "Data Security Management Measures*," (Draft for Comment*)*, New America (May 31, 2019), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-draft-data-security-management-measures/.

[102] *Id.* at EB-PUBLIC-919 (2019 Draft Data Security Management Measures, Article 36).

[103] *Id.* at EB-PUBLIC-917 (2019 Draft Data Security Management Measures, Article 15).

[104] *Id.* at EB-PUBLIC-919 (2019 Draft Data Security Management Measures, Article 37).

efforts *wherever they are in the world*."[105] As the Commission noted in its 2019 *China Mobile* Order:

> Article 7 of the 2017 National Intelligence Law provides '[a]n organization or citizen shall support, assist in and cooperate in national intelligence work in accordance with the law and keep confidential the national intelligence work that it or he knows. Article 14 permits Chinese intelligence institutions to request citizens and organizations to provide necessary support, assistance, and cooperation. Article 17 allows Chinese intelligence agencies to take control of an organization's facilities, including communications equipment.[106]

The Commission has also identified other PRC laws that "obligate citizens and organizations to cooperate with intelligence activities."[107] The 2017 Intelligence Law, if applied in concert with the 2017 Cybersecurity Law, provides the PRC government far more specific authority to access and regulate many features of corporate networks (inside as well as outside of China) that might be useful for intelligence gathering.[108]

In May 2020, the PRC's National People's Congress (NPC) announced that it would unilaterally and arbitrarily impose national security legislation on Hong Kong.[109] Although the

---

[105] *China Mobile Int'l (USA) Inc.,* Memorandum Opinion and Order, 34 FCC Rcd 3361, 3369, ¶ 17 (2019) (emphasis added). *See also* Exhibit 47 at EB-PUBLIC-925, Carolina Dackö and Lucas Jonsson, *Applicability of National Intelligence Law to Chinese and non-Chinese Entities,* Mannheimer Swartling (Jan. 2019), https://www.mannheimerswartling.se/globalassets/nyhetsbrev/msa_nyhetsbrev_national-intelligence-law_jan-19.pdf; Exhibit 48 at EB-PUBLIC-931, *National Intelligence Law of the People's Republic,* National People's Congress, (last visited Mar. 24, 2020), https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf (Google's cache of http://www.npc.gov.cn/npc/xinwen/2017-06/27/content_2024529.htm as it appeared on Mar. 25, 2019, 5:27:04 GMT).

[106] *China Mobile,* 34 FCC Rcd at 3369, ¶ 17 (footnotes omitted)

[107] *Id.* at n.56.

[108] Exhibit 41 at EB-PUBLIC-850.

[109] *See* Exhibit 130 at EB-PUBLIC-2348, P.R.C. National People's Congress Proposal on Hong Kong National Security Legislation, U.S. Dep't of State (May 27, 2020) (Statement of Secretary of State Michael R. Pompeo), https://www.state.gov/prc-national-peoples-congress-proposal-on-hong-kong-national-security-legislation/. *See also* Exhibit 131 at EB-PUBLIC-2352, 2020 Hong

details of the legislation are not yet clear, the NPC's proposal cited the possibility for mainland security organs to set up agencies in Hong Kong when needed.[110] Given these and other actions by the PRC government, the Secretary of State decided to certify that Hong Kong does not continue to warrant differential treatment vis-à-vis mainland China under U.S. law.[111] Since 2019, the PRC government has endeavored to undermine Hong Kong's high degree of autonomy, democratic institutions, and civil liberties that were guaranteed to it by the Sino-British Declaration and the Basic Law.[112]

The Hong Kong Basic Law provides some limited protections for the application of PRC law within Hong Kong.[113] Although the Basic Law sets forth the general principle that PRC laws would not be applied in Hong Kong, the Standing Committee of the National People's Congress is empowered to designate specific PRC laws that may be applied in Hong Kong.[114] Such laws must "relat[e] to defen[s]e and foreign affairs" or other matters specified in the Basic

---

Kong Policy Act Report, U.S. Dep't of State (May 28, 2020), https://www.state.gov/2020-hong-kong-policy-act-report/; Exhibit 128 at EB-PUBLIC-2344, *China adopts decision to make Hong Kong national security laws*, Xinhua (May 28, 2020), http://www.xinhuanet.com/english/2020-05/28/c_139096394.htm; Exhibit 129 at EB-PUBLIC-2346*, Only national security legislation can bring Hong Kong lasting security***,** Xinhua (May 27, 2020), http://www.npc.gov.cn/englishnpc/c23934/202005/aaa0ccb8145c48b0adaf860b054360cf.shtml.

[110] *See* Exhibit 128 at EB-PUBLIC-2344.

[111] *See* Exhibit 130 at EB-PUBLIC-2348.

[112] Exhibit 131 at EB-PUBLIC-2353; Exhibit 124 at EB-PUBLIC-2139, The Sino-British Joint Declaration, United Kingdom of Great Britain and Northern Ireland and the People's Republic of China, Dec. 19, 1984, https://www.cmab.gov.hk/en/issues/joint.htm; Exhibit 125 at EB-PUBLIC-2171, Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China, Article 2 (effective July 1, 1997) (hereinafter *Hong Kong Basic Law*), https://www.basiclaw.gov.hk/en/basiclawtext/images/basiclaw_full_text_en.pdf.

[113] *See* Exhibit 125 at EB-PUBLIC-2171, *Hong Kong Basic Law*.

[114] *Id.* at EB-PUBLIC-2176, *Hong Kong Basic Law*, Article 18.

Law.[115] The PRC government may also issue an order applying relevant PRC laws in Hong Kong if the Standing Committee of the National People's Congress decides to declare war, or decides that there is "turmoil" that "endangers national unity or security[.]"[116] Officially, the "power of interpretation" of the Hong Kong Basic Law is "vested in the Standing Committee of the National People's Congress."[117]

C. For commercial reasons related to increased demand, submarine cable landing stations have evolved to facilitate data-rich environments supporting global data centers and interconnections

In the context of this evolving national security landscape, there has also been an evolving technology landscape that exacerbates the national security concerns already described. New concerns have arisen due to significant disruptions in the subsea cable industry and increasing demand. According to Google, "[p]eople think that data is in the cloud, but it's not. It's in the ocean."[118] Today, the cloud revolution is happening under the ocean and is changing where data goes. Data has overtaken voice traffic in the last decade,[119] and hyperscale providers'[120] private networks today carry more traffic than the Internet's traditional backbone

---

[115] Id.

[116] Id.

[117] *Id.* at EB-PUBLIC-2219, Hong Kong Basic Law, Article 158.

[118] Exhibit 50 at EB-PUBLIC-942, Adam Satariano, *How the Internet Travels Across Oceans,* NYTimes.com (Mar. 10, 2019), https://www.nytimes.com/interactive/2019/03/10/technology/internet-cables-oceans.html (quoting Google's Jayne Stowell, who oversees construction of Google's undersea cable projects).

[119] Exhibit 56 at EB-PUBLIC-1058, Brian Lavallée, *Connecting Data Centers Under the Sea, Ciena* (Apr. 27, 2016), https://www.ciena.com/insights/articles/Connecting-Data-Centers-Under-the-Sea_prx.html.

[120] A "hyperscale provider" is defined primarily by its massive size and scalability. Hyperscale providers typically provide information technology (IT) services for millions or even billions of users. The scale of hyperscale providers' businesses requires large data centers, and their global

providers.[121] "The world of subsea communications cables, which for many years was the domain of large global telecom providers, is now being driven by the needs of the largest Internet companies."[122] To be clear, the rise of hyperscale provision of service meets the increasing demands for data and speed, and the Executive Branch does not object to businesses that have developed technology and infrastructure to meet consumer needs. What the Executive Branch seeks to highlight, however, is that these developments necessitate an update to the associated national security considerations, particularly in cases where supporting infrastructure traverses foreign jurisdictions that provide foreign entities with access to U.S. persons' data. Subsea cables are the primary conduits for transferring data between continents, and the potential that access to the subsea cables (which may include millions of Americans' sensitive personal data) may be exploited by foreign actors, are important components of that updated view. Four hyperscale providers—Google, Facebook, Microsoft and Amazon—are now the largest investors

---

scope requires a distributed network of these large data centers, and low-latency connectivity between them. The hyperscale data center is reshaping the global infrastructure for data centers and cloud computing platforms, and disrupting the business of how IT space is bought, built, and provisioned. *See* Exhibit 127 at EB-PUBLIC-2332, Rich Miller, *White Paper: Hyperscale Data Centers,* Data Center Frontier and Iron Mountain (Sept. 2019), https://datacenterfrontier.com/white-paper/hyperscale-data-centers-special-report/.

[121] Exhibit 60 at EB-PUBLIC-1089, TeleGeography, *White Paper, Subsea cables and interconnection hubs: The interplay of diversifying routes and peering markets*, DE-CIX (Jan. 2019), https://www.de-cix.net/en/about-de-cix/academy/white-papers/subsea-cables-and-interconnection-hubs-the-interplay-of-diversifying-routes-and-peering-markets. *See also* Exhibit 52 at EB-PUBLIC-955, Alan Weissberger, *Will Hyperscale Cloud Companies (e.g., Google) Control the Internet's Backbone?,* IEEE Communications Society (Apr. 25, 2019), https://techblog.comsoc.org/2019/04/25/will-hyperscale-cloud-companies-e-g-google-control-the-internets-backbone/.

[122] Exhibit 53 at EB-PUBLIC-966, Rich Miller, *Cloud Players are Redrawing the Subsea Cable Map*, Data Center Frontier (Dec. 4, 2018), https://datacenterfrontier.com/cloud-players-are-redrawing-the-subsea-cable-map/.

in new subsea cable routes.[123] In 2018 alone, Google and Facebook were estimated to have spent $39 billion on capital expenditures on network infrastructure, including submarine cables, Points of Presence (PoPs), and data centers.[124]

In the last five years alone, the hyperscale providers have re-shaped how data flows between continents. They have dramatically increased the need for global bandwidth in order to support replication between their massive proprietary data centers.[125] To speed up delivery of services to end users, hyperscale providers typically store replicas of their data in multiple data centers around the world, procuring data from the location closest to the end user.[126] According to a leading subsea cable vendor, "[w]hat Facebook, for example, is trying to achieve is a uniform user experience around the world [. . . .] That requires the free movement of your information and your Facebook friends' information. This in turn means replication of Facebook information around different data centres, and that's what drives Facebook's bandwidth needs and the kind of cable they want to fund."[127]

---

[123] *Id.;* Exhibit 54 at EB-PUBLIC-983, Vinay Nagpal and Erick Contag, *Convergence of Data Centers, Subsea, and Terrestrial Fiber*, Pacific Telecommunications Council (Sept. 19, 2019), https://www.ptc.org/20190/09/convergence-of-data-centers-subsea-and-terrestrial-fiber/.

[124] Exhibit 55 at EB-PUBLIC-997, Tim Stronge, Jon Hjembo, Brianna Boudreau, *TeleGeography at PTC 2020,* TeleGeography (Jan. 19, 2020), https://www2.telegeography.com/ptc-2020 (Presentation: How much growth is too much growth?).

[125] Exhibit 56 at EB-PUBLIC-1058 to -60.

[126] Exhibit 57 at EB-PUBLIC-1071, Jeff Hecht, *The Bandwidth Bottleneck that is Throttling the Internet*, Nature (Aug. 10, 2016), https://www.nature.com/news/the-bandwidth-bottleneck-that-is-throttling-the-internet-1.20392.

[127] Exhibit 58 at EB-PUBLIC-1075, Guy Matthews, *Power Beneath the Surface*, Capacity (Dec. 3, 2019), https://www.capacitymedia.com/articles/3824623/power-beneath-the-surface (quoting Geoff Bennett, director, solutions and technology with vendor Infinera).

The proliferation of hyperscale data centers is the biggest driver of global bandwidth demand today, and hyperscale providers' efforts to synchronize their proprietary data centers now consume more bandwidth than public Internet traffic.[128] Recent cables, such as the trans-Atlantic MAREA cable owned by Microsoft and Facebook, were reportedly built expressly for this purpose.[129] Because data center replication, synchronization, and related applications are very sensitive to delay (latency), hyperscale providers—more so than the average bandwidth consumer—demand direct, low latency submarine cables.[130] According to a leading subsea cable vendor, "Facebook and Google know what every additional millisecond of user latency costs . . . These players know what they are doing – to two decimal place[s] of accuracy – such is their access to cutting edge analytics."[131]

Changes giving rise to hyperscale data centers have also shaped the development of subsea cable landing stations and global interconnection and peering markets.[132] Interconnection traffic is driven by businesses wishing to bypass the public Internet in favor of private channels to facilitate data exchange directly between companies and their networks. Today, there is more

[128] Exhibit 57 at EB-PUBLIC-1071.

[129] *Id*. at EB-PUBLIC-1070 to -71.

[130] Exhibit 59 at EB-PUBLIC-1084, Jeff Hecht, *Submarine cable goes for record: 144,000 Gigabits from Hong Kong to L.A. in 1 Second*, IEEE Spectrum (Jan. 3, 2018), https://spectrum.ieee.org/telecom/internet/submarine-cable-goes-for-record-144000-gigabits-from-hong-kong-to-la-in-1-second ("One tactic is to divide long cables into shorter, island-hopping segments, which could offer more bandwidth by virtue of the power that could be injected at the junction points. But that's not attractive to Internet giants, which want direct, low-latency routes between their data centers.").

[131] Exhibit 58 at EB-PUBLIC-1075, (quoting Geoff Bennett, director, solutions and technology with vendor Infinera).

[132] Exhibit 60 at EB-PUBLIC-1087.

private interconnection traffic than public Internet traffic.[133] Changing requirements in the subsea cable market have impacted how cable landing stations are designed. Traditionally, a subsea cable landed in an isolated facility near a beach and relied on a single carrier to bring cable traffic to meet terrestrial networks. Subsea cable stations today are located inland far from the beach, and cables now terminate directly inside data centers.[134] These new cable landing stations attract Internet exchanges and private peering, providing many more options for interconnections to multiple terrestrial networks than was previously available. Subsea cable infrastructure provides an attractive interconnection ecosystem, with the close, direct, and many-to-many global connectivity that is the essence of interconnection.[135] As a result, submarine

[133] *Id.; see also* Exhibit 61 at EB-PUBLIC-1114, Daniel S. Hamilton and Joseph P. Quinlan, *The Transatlantic Economy 2019,* Foreign Policy Institute (2019) (Chapter 3—From Pipes to Platforms: The Transatlantic Digital Economy), https://transatlanticrelations.org/wp-content/uploads/2019/03/TE2019_Chapter-3.pdf.

[134] Exhibit 54 at EB-PUBLIC-983 ("Over the past few years, we have also witnessed a shift in how systems are built. Early systems were designed from one Cable Landing Station (CLS) to the next – a CLS-to-CLS design – where the subsea network met the terrestrial network for onward connectivity. As carrier-neutral city-center POPs emerged, . . . system designs started a POP-to-POP shift. Today's trend, however, aims to connect DC-to-DC [data center to data center], in some cases replacing the traditional CLS, with smaller modular CLSs to house Power Feed Equipment (PFE) and push out Subsea Line Terminal Equipment (SLTE) to the data center or a connectivity-rich, carrier-neutral interconnection colocation facility."). *See also* Exhibit 58 at EB-PUBLIC-1076 ("Traditionally you would have had the cable itself underwater, and the terminals within the landing stations . . . Now these terminals are typically pushed right into the data centres. With the majority of new traffic being turned up being from Google, Facebook, Microsoft and other content players.") (quoting Brian Lavallée, vendor Ciena's senior director of portfolio marketing and an expert in submarine networking solutions).

[135] Exhibit 54 at EB-PUBLIC-984 ("The landing of subsea cables in a data center is a trend that is continuing to gain traction in multiple geographies around the world, leading to the development of subsea interconnection ecosystems in carrier-neutral data centers"); Exhibit 61 at EB-PUBLIC-1114 ("[Businesses] need interconnection, and the expansion of submarine cable infrastructure offers just that. Subsea cables bring companies to the digital edge, and the ability to land the cables directly inside data centers enables these systems to deliver the close, direct, many-to-many global connectivity that is the essence of interconnection.").

cable landing stations today are significant data-rich environments, and are influential new players in the global data center and interconnection markets.

V. The Executive Branch recommends partial denial with respect to PLCN's Chinese owners, Hong Kong based-majority owner Pacific Light Data and Chinese parent entity Dr. Peng Group, and with respect to PLCN's Hong Kong landing site

A. The Executive Branch recommends denying the license application with respect to Hong Kong-based Pacific Light Data and PRC parent entity Dr. Peng Group

Applicant Pacific Light Data is a Hong Kong-based company founded in 2015.[136] Pacific Light Data is an indirect subsidiary of Dr. Peng Telecom & Media Group Co., Ltd. (Dr. Peng Group), a publicly traded company based in Chengdu, China.[137] Dr. Peng Group indirectly owns [redacted] percent interest in Pacific Light Data.[138] China Culture Silicon Valley Co. Ltd. has approximately a [redacted] percent interest in Pacific Light Data.[139] [redacted][140] A third company, [redacted][141] [redacted],[142] [redacted]

---

[136] *See* Exhibit 100 at EB-PUBLIC-1733, Amendment to Application for a Cable Landing License, SCL-AMD-20171227-00025, Appendix D at 1 (Dec. 27, 2017) (hereinafter *PLCN Application Amendment*).

[137] *Id.* at EB-PUBLIC-1733 to -34.

[138] *See id.* at EB-PUBLIC-1734 (identifying Dr. Peng Group, China Culture Silicon Valley Limited as owners of Pacific Light Data); Exhibit 2003 at CONF-PLDC-30, (originally produced as PLCN-000939) (identifying Dr. Peng Group as holding [redacted] ownership of Dr. Peng Holding Hong Kong Limited, which in turns holds [redacted] of PLD Holdings Limited, which in turn holds [redacted] percent of Pacific Light Data).

[139] Exhibit 2003 at CONF-PLDC-30 (originally produced as PLCN-000939) [redacted].

[140] Id.

[141] The Executive Branch has not found any information about [redacted]

[142] Exhibit 2003 at CONF-PLDC-30 (originally produced as PLCN-000939).

[redacted].[143]

Pacific Light Data has a complex ownership history. It is a newcomer to the industry, and PLCN is its first project.[144] Pacific Light Data's original investor and owner was China Soft Power Technology Holdings Ltd., a Bermuda company listed in Hong Kong that, according to Hong Kong corporate registry data, has been dormant since December 1999 and has changed its name over a dozen times since 2015.[145] The company reported over $100 million in losses and negligible revenue for the fiscal year ending in March 31, 2016.[146]

[143] 47 C.F.R. § 1.767(h)(2).

[144] Exhibit 100 at EB-PUBLIC-1733. *See also* Exhibit 63 at EB-PUBLIC-1125, Drew FitzGerald, *Google, Facebook to Invest in U.S.-China Data Link,* Wall Street Journal (Oct. 12, 2016) ("Pacific Light Data is a newcomer to the industry with no previous experience building networks.").

[145] Exhibit 64 at EB-PUBLIC-1127, Company Name Search, Integrated Companies Registry Information System (ICRIS), Companies Registry—Government of Hong Kong (last visited Mar. 7, 2020) (results of search for "China Soft Power"); Exhibit 66 at EB-PUBLIC-1139, *Name Change, Change of Stock Short Name and Company Website,* China Jinhai International Group Limited (Dec. 4, 2014), http://doc.irasia.com/listco/hk/centralwealth/announcement/a141204.pdf (disclosing name change from "ICube Technology Holdings Limited" to "China Jinhai International Group Limited"); Exhibit 67 at EB-PUBLIC-1142, *Name Change, Changes of Stock Short Name and Company Website,* China Soft Power Technology Holdings Limited (Aug. 13, 2015), http://doc.irasia.com/listco/hk/centralwealth/circulars/c150813.pdf (disclosing name change from "China Jinhai International Group Limited" to "China Soft Power Technology Holdings Limited"); Exhibit 68 at EB-PUBLIC-1145, *Name Change, Changes of Stock Short Names and Company Website,* Central Wealth Group Holdings Limited (disclosing name change from "China Soft Power Technology Holdings Limited" to "Central Wealth Group Holdings Limited"); *see also* Exhibit 65 at EB-PUBLIC-1131, *Some Hong Kong companies change their name every couple months; Data Guru exposes the worst culprits*, dataguru.hk (Dec. 24, 2018), https://blog.dataguru.hk/2018/12/24/some-hong-kong-companies-change-their-name-every-couple-of-months-why/.

[146] Exhibit 63 at EB-PUBLIC-1125; Exhibit 105 at EB-PUBLIC-1810, *2015-16 Annual Report* at 4, China Soft Power Technology Holdings Limited (June 22, 2016), https://doc.irasia.com/listco/hk/centralwealth/annual/2016/ar2016.pdf.

In March 2016, all interests in Pacific Light Data were acquired by China Culture Silicon Valley Limited, a Hong Kong-based company wholly owned by Wei Junkang, who is the father of the chairman of the original investor (Wei Zhenyu, chairman of China Soft Power Technology Holdings).[148] China Culture Silicon Valley appears to be a holding company that has not

[147] Derived from Exhibit 2003 at CONF-PLDC-30 (originally produced as PLCN-000939); Exhibit 72 at EB-1162, *Connected Transaction: Disposal of Entire Interest in PLD Holdings Limited*, China Soft Power Technology Holdings Limited (Mar. 31, 2016), https://doc.irasia.com/listco/hk/centralwealth/announcement/a160331.pdf.

[148] Exhibit 72 at EB-1162. Months later, China Soft Power Technology Holdings reported disposing its remaining assets in a transaction that involved Mr. Wei Zhenyu and his step-mother, Ms. He Xin; Ms. He represented the purchaser, a business venture supported by the China Youth Concern Committee, an organization established under the Central Committee of the Communist Party of China. *See* Exhibit 73 at EB-PUBLIC-1175 to -76, *Discloseable and Connected Transaction: Disposal of Entire Interest in CPST Holdings Limited, Proposed Re-election of Director and Notice of Special General Meeting*, China Soft Power Technology Holdings Limited (Aug. 3, 2016),

conducted any business other than investing in Pacific Light Data.[149] In December 2017, Dr. Peng Group acquired a 93 percent ownership interest in Pacific Light Data and China Culture Silicon Valley retained a 7 percent interest.[150] In February 2019, [redacted] acquired a [redacted] percent interest in China Culture Silicon Valley.[151]

Although Pacific Light Data was a relative newcomer to the industry, within one year of incorporation, it:

- reportedly made the decision to build PLCN within two months;[152]
- invested in a $10 million route study because a direct U.S.-Hong Kong submarine cable had never been built before;[153]

---

https://doc.irasia.com/listco/hk/centralwealth/circulars/c160802.pdf.

[149] *See, e.g.,* Exhibit 106 at EB-PUBLIC-1973, Winston Qiu, Dr. Peng Acquires PLCN (鹏博士发布收购PLCN海缆项目公告), Submarine Cable Networks (Dec. 11, 2017), https://www.submarinenetworks.com/zh/cables/dr-peng-acquires-plcn (Google translation stating "In addition to investing in [Pacific Light Data], CCSV [China Culture Silicon Valley] does not carry out other business.") (Attachment E to Team Telecom's Third Set of Follow-up Questions to Pacific Light Data, sent Oct. 4, 2019). *See also* Exhibit 2003 at CONF-PLDC-40 (certified translation of "Appendix [sic] E," website at https://www.submarinenetworks.com/zh/cables/dr-peng-acquires-plcn, provided by Pacific Light Data, originally produced as PLCN-000949).

[150] Exhibit 100 at EB-PUBLIC-1734, *PLCN Application Amendment* at 2.

[151] Exhibit 2001 at CONF-PLDC-2, 4 (originally produced as PLCN-000541, -543).

[152] Exhibit 69 at EB-PUBLIC-1149, Winston Qiu, *Invader to Build Pacific Light Cable Network Connecting Hong Kong and the US,* Submarine Cable Networks (Nov. 16, 2015), https://www.submarinenetworks.com/en/systems/trans-pacific/plcn/invader-to-build-pacific-light-cable-network-connecting-hong-kong-and-the-us; *see also* Exhibit 71 at EB-PUBLIC-1160, Comms Update, *Cable Compendium: a guide to the week's submarine and terrestrial developments,* TeleGeography (Nov. 20, 2015), https://www.commsupdate.com/articles/2015/11/20/cable-compendium-a-guide-to-the-weeks-submarine-and-terrestrial-developments/.

[153] Exhibit 70 at EB-PUBLIC-1154, *Inside Information, Entering into the Memorandum of Understanding and the Professional Services Agreement*, China Soft Power Technology Holdings Limited (Nov. 13, 2015), https://doc.irasia.com/listco/hk/centralwealth/announcement/a151113.pdf.

- agreed to negotiate a supply contract estimated at $400 million to build PLCN;[154]
- decided that PLCN would use advanced optical technology, including spectrum bands (C+L band) that had never been deployed in a submarine cable before;[155]
- allocated for itself 96 Tbps design capacity on PLCN, more than 1.5 times the existing record on a trans-Pacific route (60 Tbps on Google's FASTER cable) and;[156]
- entered into a partnership with Google and Facebook on PLCN.[157]

In addition to Pacific Light Data's origins, which obscure the identity of the original beneficial owner that provided PLCN's initial funding, Pacific Light Data's and its parent Dr. Peng Group's support for the PRC government's One Belt, One Road and Digital Silk Road initiatives raise national security concerns.

1. Parent Entity Dr. Peng Group supports the PRC government's infrastructure goals, has business relationships with PRC intelligence and security services, and is subject to PRC national security and intelligence laws

Dr. Peng Group is a telecommunications company based in Chengdu, China.[158] It is the largest privately owned telecommunications provider in China, with more than 38,000 employees, and is the fourth-largest telecommunications company after the three Chinese telecommunications state-owned enterprises (China Mobile, China, Telecom, and China

[154] *Id.*; Exhibit 71 at EB-PUBLIC-1160.

[155] Exhibit 70 at EB-PUBLIC-1154; Exhibit 59 at EB-PUBLIC-1082.

[156] Exhibit 70 at EB-PUBLIC-1154; *see also* Exhibit 59 at EB-PUBLIC-1082.

[157] Exhibit 63 at EB-PUBLIC-1124.

[158] *See* Exhibit 100 at EB-PUBLIC-1734.

Unicom).[159] Dr. Peng Group is listed on the Shanghai Stock Exchange and focuses its business on Internet access, Internet data centers, and cloud computing services.[160]

a) Dr. Peng Group and the PRC government's One Belt, One Road initiative.

Dr. Peng Group has claimed that the PLCN project was in line with the objectives of the One Belt, One Road initiative,[161] stating that its acquisition of Pacific Light Data was "[redacted]."[162] Dr. Peng has cited as one of its "Competitive Strengths" the fact that it is "[w]ell [p]ositioned to [b]enefit from [f]avourable [n]ational [s]trategies and [i]ndustry [p]olicies," such as PRC policies to develop big data, cloud computing, and Internet of Things capabilities.[163] The purpose of Dr. Peng Group's acquisition of Pacific Light Data [redacted]."[164]

[159] Exhibit 74 at EB-PUBLIC-1232, -38, -51, -71, *Offering Memorandum,* Dr. Peng Telecom & Media Group Co., Ltd. (May 25, 2017), https://links.sgx.com/FileOpen/DrPHHL_Offering%20Memorandum%20dated%2025%20May%202017.ashx?App=Prospectus&FileID=31941 (excerpts of relevant portions).

[160] *Id.* at EB-PUBLIC-1232, -38.

[161] Exhibit 106 at EB-PUBLIC-1974 (Google translation stating that the PLCN project "is in line with the 'One Belt, One Road' national strategy").

[162] Exhibit 2003, CONF-PLDC-41 (originally produced as PLCN-000949).

[163] Exhibit 74 at EB-PUBLIC-1253.

[164] Exhibit 2003 at CONF-PLDC-27 (originally produced as PLCN-000936).

b) Dr. Peng Group and PRC government intelligence and security services.[165]

When asked by Team Telecom whether it had contracts with any PRC government intelligence and security services, Dr. Peng Group stated that it [redacted][166] [redacted][167] [redacted][168] [redacted][169]

c) Dr. Peng Group and Huawei[170]

When asked by Team Telecom about its relationship with Huawei, Dr. Peng Group stated that it [redacted][171] Dr. Peng Group's relationship with Huawei was described in the press as a "strategic cooperation agreement with Huawei to jointly research cloud computing, artificial intelligence and 5G mobile technology[.]"[172] A December 2019 State Department publication noted that "Huawei has deep ties to the Chinese Communist Party and

[165] Exhibit 75 at EB-PUBLIC-1291, Kate O'Keeffe, Drew FitzGerald, and Jeremy Page, *National Security Concerns Threaten Undersea Data Link Backed by Google, Facebook,* Wall Street Journal (Aug. 28, 2019).

[166] Exhibit 2003 at CONF-PLDC-23 (originally produced as PLCN-000932).

[167] Id.

[168] Id.

[169] *Id.* at CONF-PLDC-24 (originally produced as PLCN-000933).

[170] Exhibit 75 at EB-PUBLIC-1291.

[171] Exhibit 2003 at CONF-PLDC-23 (originally produced as PLCN-000933].

[172] Exhibit 75 at EB-PUBLIC-1291.

military."[173] In November 2019, the Attorney General issued a letter to the Chairman of the FCC explaining that Huawei cannot be trusted.[174] In October 2012, the House Permanent Select Committee of Intelligence (HPSCI) determined that "Huawei . . . cannot be trusted to be free of foreign state influence and thus pose[s] a security threat to the United States and to our systems."[175] Huawei has since been the subject of longstanding national security concerns within the U.S. government.[176] In January 2020, the Commission prohibited the use of Universal Service Fund (USF) funds to purchase or obtain equipment or services provided by Huawei due to national security concerns.[177] Huawei is also under multiple federal criminal indictments in the United States.[178] These relationships raise further questions about Dr. Peng Group's being subject to influence and control that would damage national security.

d) Dr. Peng Group is subject to PRC laws that require Chinese entities to

---

[173] Exhibit 118 at EB-PUBLIC-2113, 5G Security—Huawei Factsheet, U.S. Dept. of State (Dec. 2019), https://policystatic.state.gov/uploads/2019/12/5G-Myth_Fact4.pdf

[174] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs,* FCC Dkt. No. WC 18-89, Letter from Attorney General William Barr (Nov. 13, 2019) https://ecfsapi.fcc.gov/file/11130351518674/Attorney%20General%20Letter%20FCC%20Docket%2018-89.pdf

[175] Exhibit 117 at EB-2057 to -58, Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger, H. Permanent Select Comm. on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, U.S. House of Representatives, 112th Cong. (Oct. 8, 2012) (hereinafter *2011 HPSCI Report*).

[176] *See, e.g., Huawei Techs. USA, Inc. v. United States*, No. 4:19-CV-159, 2020 WL 805257, at *1-*7 (E.D. Tex. Feb. 18, 2020) (citing national security concerns expressed by the U.S.-China Economic and Security Review Commission, House Permanent Select Committee on Intelligence, Federal Bureau of Intelligence, and others).

[177] Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, 85 Fed. Reg. 230 (Jan. 1, 2020) (FCC final rule prohibiting use of Universal Service Fund funds to purchase or obtain equipment or services provided by Huawei).

[178] Exhibit 76 at EB-PUBLIC-1293, Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charged in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets, U.S. Dep't of Justice (Feb. 13, 2020), https://www.justice.gov/opa/pr/chinese-telecommunications-

support Beijing's security agencies

Dr. Peng Group has stated that it is [redacted] [179] When asked whether it agreed with the Commission's understanding that Chinese law compelled its citizens and organizations to assist PRC intelligence anywhere in the world,[180] Dr. Peng Group [redacted]

[redacted]

conglomerate-huawei-and-subsidiaries-charged-racketeering; Exhibit 77 at EB-PUBLIC-1296, United States v. Huawei Technologies Co., Ltd., et al., Cr. No. 18-457, ECF No. 126, Superseding Indictment (E.D.N.Y. Feb. 13, 2020); United States v. Huawei Device Co., Ltd. et al., Cr. No. 19-010, ECF No. 1, Indictment (W.D. Wash. Jan. 16, 2019).

[179] Exhibit 2003 at CONF-PLDC-27 to -28 (originally produced as PLCN-000936 to -37).

[180] *See China Mobile,* 34 FCC Rcd at 3369, ¶ 17.

[181] Exhibit 2003 at CONF-PLDC-28 (originally produced as PLCN-000937).

[182] *Id*.

[183] *Id*.

[redacted]

2. Dr. Peng Group may have failed to comply with U.S. law in acquiring U.S. telecommunications companies, raising questions about its trustworthiness

In 2016, reports stated that Dr. Peng Group acquired 100 percent equity in Vertex Group and related companies (collectively, Vertex) for $9 million.[184] In a securities filing for the Vertex acquisition, Dr. Peng Group stated that [redacted][185] At the time, Vertex Telecom and Vertex SSX were California-based companies holding FCC international common carrier authorizations under Section 214 of the Communications Act of 1934, as amended.[186] Under U.S. law and FCC regulations, Dr. Peng Group would have been required to

[184] Exhibit 74 at EB-PUBLIC-1235; Exhibit 113 at EB-PUBLIC-2003, *BRIEF-Dr Peng Telecom and Media's unit to acquire Vertex Group and related companies,* Reuters (Apr. 30, 2015), https://www.reuters.com/article/idUSL4N0XR2K420150430.

[185] Exhibit 2003 at CONF-PLDC-35 (originally produced as PLCN-000944).

[186] *See* Exhibit 107 at EB-PUBLIC-1986 (Google translation stating that "Vertex . . . and affiliated companies . . . hold . . . US Federal Communications Commission FCC-214 license") (attached as Exhibit C to Team Telecom's Third Set of Follow-up Questions to Pacific Light Data, sent Oct. 4, 2019); *see also* Exhibit 2003 at CONF-PLDC-32 (certified translation provided by Pacific Light Data, originally produced as PCLN-000942). *See also FCC International Section 214 Current Authorizations List,* FCC International Bureau (last visited Mar. 24, 2020), https://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr029b.hts?as_subsystem_code=ITC/INTERNATIONAL+SECTION+214&column=V_SITE_ANTENNA_FREQ.file_numberC/FILE+NUMBER&fstate=1/CURRENT&prepare=.

receive Commission approval before taking control of Vertex and its telecommunications facilities.[187] Dr. Peng Group's reported acquisition of Vertex would likely have been referred to the Executive Branch, including Team Telecom, to review for any national security and law enforcement concerns. When asked by Team Telecom about the Vertex acquisition, Dr. Peng Group stated [redacted][188] [redacted]. Dr. Peng Group, as a sophisticated, publicly traded company on the Shanghai Stock Exchange, had previously applied for an international Section 214 authorization for another subsidiary; thus, it either knew or should have known of its legal requirement to seek Commission review.[189] Moreover, Vertex had operated with an international Section 214 authorization for more than a decade and also either knew or should have known the Commission's requirements.[190]

---

[187] 47 U.S.C. § 214 ("No carrier . . . shall acquire or operate any line, . . . unless and until there shall first have been obtained from the Commission a certificate that the present or future public convenience and necessity require" it); 47 C.F.R. § 63.24 ("an international section 214 authorization may be assigned, or control of such authorization may be transferred by the transfer of control of any entity holding such authorization . . . *only upon application to and prior approval by the Commission*") (emphasis added).

[188] Exhibit 2003 at CONF-PLDC-15 (originally produced as PLCN-000924).

[189] *See International Section 214 Application, FCC Form 214,* ITC-214-20150417-00095 (Apr. 17, 2015) (application filed by GW-Mobile, Inc.). *See also FCC Form 499 Filer Database,* Dr. Peng Holding Inc. (last visited Mar. 24, 2020), http://apps.fcc.gov/cgb/form499/499detail.cfm?FilerNum=830473 (identifying Dr. Peng Holding Inc., formerly known as GW-Mobile, Inc.); Exhibit 2003 at CONF-PLDC-15 (originally produced as PLCN-000924).

[190] Exhibit 80 at EB-PUBLIC-1408, *Selected Application Listing By File Number*, FCC File Number ITC-214-19980226-00152, FCC International Bureau (last visited Mar. 18, 2020)

Dr. Peng Group has also made inconsistent statements about its connection to the acquisition of a Houston-based ICT company, EnTouch Systems, Inc., by "Acme Communications, Inc." that raise further questions about Dr. Peng Group's trustworthiness and the intent of its employees.[191]

In March 2019, Team Telecom referred Dr. Peng Group's reported acquisitions of Vertex Group and allegations of its involvement in Acme Communications' acquisition of EnTouch to the Commission's International Bureau.

3. Pacific Light Data has significant connections to PRC state-owned carrier China Unicom

Pacific Light Data's significant connections to PRC state-owned carrier China Unicom raise concerns that the PRC government could exercise significant control over Pacific Light Data through new laws that allow it to compel assistance, support, or cooperation from any PRC

(search for "Vertex Group ").

[191] *Compare* Exhibit 78 at EB-PUBLIC-1352, *Entouch Systems, Inc. v. J. Lyn Findley,* C.A. No. 2018-0817-KSJM, Defendant's Answer, Affirmative Defenses, and Verified Counterclaim (Del. Ch. Ct. Jan. 14, 2019) (alleging Dr. Peng Group's involvement in "Fraud against the United States Government") *with* Exhibit 2003 at CONF-PLDC-13 to -22 (originally produced as PLDC-000922 to -31). *See also* Exhibit 79 at EB-PUBLIC-1375, *J. Lyn Findley v. enTouch Systems, Inc.,* Case No. 2018-65570, Plaintiff's Original Petition (Tex. Dist. Ct. filed Sept. 18, 2018); Exhibit 114 at EB-PUBLIC-2005, *Entouch Systems, Inc. v. J. Lyn Findley,* C.A. No. 2018-0817-KSJM, Stipulation of Dismissal with Prejudice (Del. Ch. Ct. Feb. 26, 2020); Exhibit 81 at EB-PUBLIC-1411, Yongzhe Jin Profile, LinkedIn (last visited May 14, 2019), https://www.linkedin.com/in/yongzhe-jin-80b2b67/?originalSubdomain=cn; Exhibit 2003 at CONF-PLDC-20 (originally produced as PLCN-000929); Exhibit 110 at EB-PUBLIC-1995, Federal Corporation Information, Dr. Peng Holding Canada, Inc., Government of Canada (last visited Mar. 24, 2020) https://www.ic.gc.ca/app/scr/cc/CorporationsCanada/fdrlCrpDtls.html?corpId=10480975; Exhibit 2001 at CONF-PLDC-6, -8, -9, May 2019 Responses to Triage Questions received from all PLCN Applicants, Appendix 12 and 13, Pacific Light Data Communication Co., Ltd., Ownership Information and Personal Identifiable Information (originally produced as PLCN-000545, -547, -548).

citizen or organization connected to Pacific Light Data. The Commission recently ordered China Unicom's U.S. subsidiary to show cause why the Commission should not initiate a proceeding to revoke its existing FCC authorizations to provide certain telecommunications services.[192] The Commission stated that the findings in its 2019 *China Mobile* denial order "raise questions regarding the vulnerability of authorization holders that are subsidiaries of a Chinese state-owned enterprise to the exploitation, influence, and control of the Chinese government."[193] The Commission noted that China Unicom's U.S. subsidiary, like the applicant in *China Mobile*, was ultimately owned and controlled by the Chinese government.[194]

First, Pacific Light Data's leadership—its chief executive officer, executive vice president and senior vice president—comes exclusively from China Unicom or its subsidiaries.[195] CEO Troy Yunfeng Li worked for China Unicom and its predecessor China Netcom for nearly 15 years before joining Pacific Light Data in December 2015.[196] At China Unicom, Mr. Li held high-level positions as "Director of Global Network" and "Director of Oversea Operation."[197] Executive Vice President Eric Liu held a high-level position (Senior Vice President of Global Wholesale) at China Unicom, focusing on developing data center and

---

[192] *China Unicom (Americas) Operations Limited,* Order to Show Cause, GN Docket 20-110, ITC-214-20020728-00361, ITC-214-20020724-00427 (rel. Apr. 24, 2020), https://licensing.fcc.gov/myibfs/download.do?attachment_key=2290860.

[193] *Id.* at 4, ¶ 6.

[194] Id.

[195] China Unicom includes China United Networks Communications Group Co. Ltd., a PRC state-owned carrier, as well as its subsidiaries such as China Unicom Global Ltd.

[196] Exhibit 82 at EB-PUBLIC-1415, Troy Yunfeng Li Profile, LinkedIn (last visited May 14, 2019), https://www.linkedin.com/in/troy-yunfeng-li-07945456/. *See also* Exhibit 2003 at CONF-PLDC-24 (originally produced as PLCN-000933).

[197] Exhibit 82 at EB-PUBLIC-1415. S*ee also* Exhibit 2003 at CONF-PLDC-24 (originally produced as PLCN-000933).

managed services business.[198] Mr. Liu previously worked for the Chinese Ministry of Foreign Affairs as "Government Relations Officer of Diplomatic Missions."[199] Senior Vice President Winston Qiu worked for China Unicom for nearly a decade, where he was a "strategic IP peering negotiator for China Unicom AS4837."[200]

Second, Pacific Light Data, as the Hong Kong landing party for PLCN, hired PCCW Global (HK) Ltd. to provide landing services for PLCN.[201] [redacted] .[202] China Unicom has at least an 18 percent ownership interest in and overlapping board membership with PCCW Ltd, the parent entity of PCCW Global (HK) Ltd.[203]

Third, Dr. Peng Group [redacted]

---

[198] Exhibit 83 at EB-PUBLIC-1418, Eric Liu Profile, LinkedIn (last visited May 14, 2019), https://www.linkedin.com/in/eric-liu-47b10914/; *see also* Exhibit 2003 at CONF-PLDC-25 (originally produced as PLCN-000934).

[199] Exhibit 83 at EB-PUBLIC-1419.

[200] Exhibit 85 at EB-PUBLIC-1428, Winston Qiu, *Next Steps in the Pacific: A Subsea Cable Changing Internet and Cloud Infrastructure Across the Pacific,* Submarine Telecoms Forum 34 (May 2018). *See also* Exhibit 84 at EB-PUBLIC-1422, Winston Qiu Profile, LinkedIn (last visited June 11, 2019), https://www.linkedin.com/in/winston-qiu-8946973b/; Exhibit 2003 at CONF-PLDC-25 (originally produced as PLCN-000934).

[201] Exhibit 103 at EB-PUBLIC-1786, Third Supplement to Application for a Cable Landing License (Streamlined Processing Requested), SCL-LIC-20170421-00012 (filed Oct. 26, 2017) (hereinafter PLCN Application Third Supplement).

[202] Exhibit 1002 at CONF-PLCN-ALL-33 to -34, May 2019 Responses to Triage Questions received from all PLCN Applicants, Appendix 2 (originally produced as PLCN-000388 to -389).

[203] Exhibit 87 at EB-PUBLIC-1459, -1516, -1598, *Annual Report 2018,* PCCW (2018), http://www.pccw.com/staticfiles/PCCWCorpsite/About%20PCCW/Investor%20Relations/Announcements%20&%20Notices/2019/Apr/2018-pccw-annual-report.pdf.

[redacted].[204] It has also expressed a "willingness to cooperate" with China Unicom and an interest in partnerships with state-owned carriers after its profits in the broadband market dropped significantly in 2018.[205]

B. The Executive Branch recommends denying the license application with respect to PLCN's connection to Hong Kong

The Executive Branch is concerned that PLCN's proposed offer of low-cost capacity to Asia through Hong Kong creates significant national security risks for the United States in the near future and provides long-term geopolitical advantages to the PRC government, especially given that PLCN represents the first of three new trans-Pacific cables that are planned to provide Hong Kong with its first direct connections to the United States.[206]

Industry market researchers have predicted that, in the next eighteen months, the market for trans-Pacific capacity would be dramatically transformed if PLCN and other planned cables enter the market with low-cost PRC-owned capacity.[207] If the Applicants' application for a connection to Hong Kong were approved, PLCN could lead the way to price declines on trans-Pacific routes, making the U.S.-Hong Kong route one of the most competitive (cheapest) ways to

---

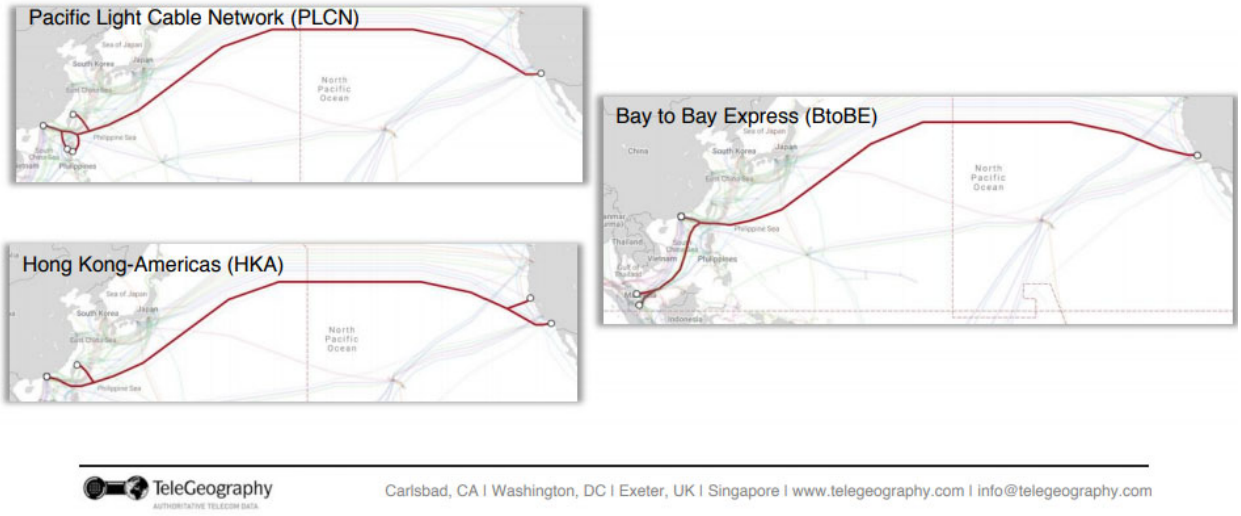
[204] Exhibit 2003 at CONF-PLDC-22 (originally produced as PLCN-000931).

[205] Exhibit 88 at EB-PUBLIC-1667, Qin Min and Zhao Runhua, *China's State-owned Carriers Edge Consumer Broadband Giant out of the Market,* Caixin Global (Apr. 2, 2019), https://www.caixinglobal.com/2019-04-02/chinas-state-owned-carriers-edge-consumer-broadband-giant-out-of-the-market-101400247.html.

[206] PLCN will be followed by the planned Hong Kong Americas (HKA) and Bay to Bay Express (BtoBE) cables, which are financed in part by the PRC government through state-owned enterprises, including China Mobile, China Telecom, and China Unicom.

[207] Exhibit 89 at EB-PUBLIC-1670, Eric Handa, *Trans-Pacific Market Capacity: Innovating and Adapting in the Face of Challenges,* Submarine Telecoms Forum 36 (May 2019).

send U.S. data to Asia.[208] This is consistent with PLCN Applicants' claims that "PLCN [w]ill [i]ncrease [c]ompetition on U.S.-Asia [r]outes . . . and lower prices[.]"[209]



TeleGeography, PTC 2020 Presentation Slide[210]

Most of PLCN's U.S. traffic would not ultimately be destined for recipients in Hong Kong or mainland Chinese users or businesses. Instead, Hong Kong would act mainly as an interconnection point for U.S. traffic to meet regional carriers serving Southeast Asia. As a result, PLCN's Hong Kong connection would increase the share of U.S. data traversing PRC territory and PRC-owned infrastructure relative to alternative existing hubs in Asia, placing such data within reach of new PRC cybersecurity and intelligence laws, raising significant national

[208] Exhibit 55 at EB-PUBLIC-1051 (slide from presentation by B. Boudreau, Pricing Update: The TG Decade Challenge, TeleGeography, Pacific Telecommunications Council 2020 (Jan. 20, 2020)).

[209] Exhibit 2 at EB-PUBLIC-8, *PLCN Application* at 4.

[210] Exhibit 55 at EB-PUBLIC-1051 (slide from presentation by B. Boudreau, Pricing Update: The TG Decade Challenge, TeleGeography, Pacific Telecommunications Council 2020 (Jan. 20, 2020)).

security concerns for the United States.[211]

1. PLCN's connection to Hong Kong would send the United States' highest-capacity pathway to Asia through PRC territory and PRC-owned infrastructure, placing U.S. data at risk of duplication and collection

PLCN alone has the highest design capacity of any subsea cable connecting the United States to Asia.[212] PLCN's 144 Tbps design capacity dwarfs that of the next largest trans-Pacific cables being used today.[213] PLCN's main trunk (a direct U.S.-Hong Kong connection) includes four fiber pairs providing 96 Tbps of design capacity that will be exclusively owned and controlled by Pacific Light Data.[214] Pacific Light Data's share alone is greater than entire cable systems that currently meet the United States' need for trans-Pacific capacity. For comparison, the NCP cable provides up to 70 Tbps and the FASTER cable provides up to 60 Tbps of design capacity.[215] [redacted].[216] Pacific Light Data has stated that it intends to offer individually negotiated wholesale capacity services on the U.S.-Hong Kong route.[217] Many users, including U.S. government agencies and contractors, may have long-term contracts with such providers and

[211] Exhibit 3 at EB-PUBLIC-47 (PLCN's Chinese-owned infrastructure includes four (out of six) fiber pairs owned by Pacific Light Data).

[212] Exhibit 2 at EB-PUBLIC-8, PLCN Application.

[213] Exhibit 3 at EB-PUBLIC-48.

[214] *Id.; see also* Exhibit 1 at EB-PUBLIC-2 to -3, *PLCN Public Notice*; Exhibit 86 at EB-PUBLIC-1430; Exhibit 99 at EB-PUBLIC-1727, *Streamlined Submarine Cable Landing License Applications, Accepted for Filing,* Public Notice, Report No. SCL-00204S (Nov. 1, 2017); Exhibit 57 at EB-PUBLIC-1070.

[215] Exhibit 59 at EB-PUBLIC-1082; Exhibit 7 at EB-PUBLIC-63, *NCP Grant Public Notice* at 3.

[216] Exhibit 2003 at CONF-PLDC-56 to -59 (originally produced as PLCN-000965 to -68).

[217] Exhibit 2 at EB-PUBLIC-7, *PLCN Application* at 3.

may be unaware that their providers may be buying wholesale capacity to Asia on PLCN. If the PLCN application were granted with a Hong Kong connection, U.S. users may find it difficult to prevent U.S. traffic from transiting Hong Kong on the way to ultimate destinations in other parts of Asia.

Google and Facebook, as minority owners of PLCN, each exclusively control a single fiber pair, providing them with 24 Tbps of design capacity per fiber pair, for a total of 48 Tbps of design capacity connecting the United States to Hong Kong via Taiwan and the Philippines.[218] Any PLCN traffic that Google and Facebook would send to Hong Kong, however, would land at the Deep Water Bay facility operated by PCCW Global (HK) Ltd. and [redacted]. As discussed earlier, PCCW Global (HK)'s parent entity, PCCW Global, has ties to China Unicom (which owns at least 18 percent of PCCW Global), including the sharing of board members.[219] In addition, Google's fiber pair would terminate in a PoP in Hong Kong provided by [redacted]

The Executive Branch's concerns are not just limited to traffic that the Applicants have reserved for their own commercial use, but also traffic that the Applicants intend to offer to other U.S. consumers and carriers "as an alternate, diverse transmission route between the [United

[218] Exhibit 85 at EB-PUBLIC-1427; Exhibit 104 at EB-PUBLIC-1800, *PLCN Commercial Operations STA*.

[219] Exhibit 103 at EB-PUBLIC-1786, *PLCN Third Application Supplement*.

[220] Exhibit 1002 at CONF-PLCN-ALL-34 (originally produced as PLCN-000389).

States] and Asia."[221] According to market research firm TeleGeography, Google's "cables will not ultimately be used only for Google traffic. What tends to happen is they will swap capacity on this cable with parties with capacity on other cables [. . . .] What effectively happens is you might see that Google has built one cable on a certain route but they can leverage that by using that as a means of exchange."[222] PLCN will also interconnect "with other submarine and terrestrial systems serving the region, [reducing] congestion on those networks and [enabling] carriers and service providers to expand their dynamic routing."[223] While such a development would be expected commercially, it also exacerbates the existing national security risk by enhancing the vulnerabilities associated with this cable and making it more likely that data intended for other destinations may pass through its systems.

The swap capacity available on PLCN to Hong Kong raises the likelihood that U.S. traffic intended for other countries in Asia may be re-routed through Hong Kong, unbeknownst to U.S. consumers and businesses. U.S. consumers of network capacity—especially those serving U.S. civilian government and military clients or contractors—may purchase capacity services through a U.S. provider and wish to avoid routing their traffic through PRC territory or on PRC-owned infrastructure. Capacity swaps on undersea cables—while a regular occurrence between network operators on subsea cables around the world—is problematic in the case of PLCN. Due to the estimated enhanced collection capabilities of the PRC in Hong Kong, any business relationship that augments traffic flow through Hong Kong gives the Executive Branch

[221] Exhibit 2 at EB-PUBLIC-9, *PLCN Application* at 5.

[222] Exhibit 90 at EB-PUBLIC-1679, Matt Burgess, *Google and Facebook are gobbling up the internet's subsea cables,* Wired UK (Nov. 18, 2018), https://www.wired.co.uk/article/subsea-cables-google-facebook (quoting Alan Mauldin, the research director for market research firm TeleGeography).

[223] Exhibit 2 at EB-PUBLIC-9, *PLCN Application* at 5.

pause. Such agreements may send U.S. traffic through Hong Kong, which raises concerns about U.S. data falling within reach of PRC laws when transiting PRC territory or PRC-owned infrastructure. If PLCN's Hong Kong connection is permitted, U.S. customers may soon have little choice but to let their traffic flow through Hong Kong in order to reach final destinations in other parts of Asia. This raises significant concerns about allowing U.S. data to fall within reach of PRC influence or PRC-owned infrastructure. Given Hong Kong's status as a regional data hub, PLCN's Hong Kong landing site could be serviced by PRC citizens and organizations, placing U.S. data within reach of entities subject to PRC law.

a) The PRC government's actions have undermined Hong Kong's autonomy from the PRC

Team Telecom asked Pacific Light Data whether it agreed with the Commission's understanding that Chinese law would require Chinese citizens and organizations to support PRC intelligence efforts wherever they are in the world.[224] Pacific Light Data stated that [redacted]

[redacted]

[224] *China Mobile,* 34 FCC Rcd at 3369, ¶ 17.

[225] Exhibit 2003 at CONF-PLDC-27 to -28 (originally produced as PLCN-000936 to -37).

[226] Id.

In November 2019, the Legislative Affairs Commission of the National People's Congress Standing Committee (NPCSC) issued a statement asserting that only the NPCSC has the power to decide whether Hong Kong laws comply with the Basic Law. This statement challenged fundamental principles of autonomy and the long-established practice of Hong Kong courts exercising the power of judicial review to adjudicate laws and review government actions.

On April 17, 2020, the PRC government's Central Government Liaison Office (CGLO) in Hong Kong issued a statement claiming that CGLO and the central government's Hong Kong and Macau Affairs Office in Beijing are not bound by a provision of the Basic Law which states that "no department of the Central People's Government . . . may interfere in the affairs" of Hong Kong.

On May 28, 2020, the National People's Congress approved a resolution to unilaterally and arbitrarily impose national security legislation on Hong Kong, a procedural step which contradicts the spirit and practice of the Sino-British Joint Declaration and the "One Country, Two Systems" framework. Consequently, on May 27, 2020, Secretary of State Pompeo certified to Congress that Hong Kong does not continue to warrant differential treatment vis-à-vis mainland China under U.S. law.[227]

2. PLCN's proposed Hong Kong connection, in combination with additional applications pending before the FCC that seek direct connections between the United States and Hong Kong, raise concerns regarding the PRC's desire to have access to an information hub with direct links to U.S. ICT infrastructure

The PRC Ministry of Industry and Information Technology (MIIT) has openly encouraged the development of subsea cables like PLCN that seek to connect Hong Kong to the United States. In 2018, MIIT's think tank, China Academy of Information and Communication

[227] Exhibit 130 at EB-PUBLIC-234. *See also* Exhibit 131 at EB-PUBLIC-2352.

Technology (CAICT), noted that "when laying future submarine cables in key directions," an important consideration was that "North America is the most important connection direction for Internet services. . . . Submarine cable construction towards the [United States] is still a major focus."[228] CAICT also encouraged PRC subsea cable policy to "[c]ontinue to play the advantage of Hong [K]ong. Hong [K]ong is an important link between China's Internet and the global Internet. Hong Kong's openness advantages can be further leveraged to proactively participate in landing submarine cable construction."[229] CAICT's policy directive expressly targeted "Internet giants such as Google, Microsoft, and Facebook" as new leading forces in the global submarine cable market, noting that "[d]ata center interconnect (DCI) has become an important goal for Internet giants in their participation in international submarine cable construction."[230] CAICT explained the motivations behind its proposed policy as the following: "the submarine cable provides information transmission channels, and data centers store and process information. To this end, *the development path of the information hub is increasingly clear*."[231]

PLCN, followed by other subsea cables financed in part by the PRC and seeking direct connections between the United States and Hong Kong, would likely lead to price declines for U.S.-Asia capacity.[232] Pacific Light Data has stated that although Hong Kong is a regional telecom hub in Asia, its global reach has been limited because its international traffic must be

[228] Exhibit 36 at EB-PUBLIC-777, *CAICT White Paper* at 24.

[229] *Id.* at EB-PUBLIC-779, *CAICT White Paper* at 26.

[230] *Id.* at EB-PUBLIC-758 to -59, *CAICT White Paper* at 5, 6.

[231] *Id.* at EB-PUBLIC-760, *CAICT White Paper* at 7 (emphasis added).

[232] Exhibit 55 at EB-PUBLIC-1051 (slide from presentation by B. Boudreau, *Pricing Update: The TG Decade Challe*nge, TeleGeography, Pacific Telecommunications Council 2020 (Jan. 20, 2020)).

routed through other intra-Asia cables, typically to Japan, before crossing the Pacific. Because PLCN will provide a direct, low latency connection between the United States and Hong Kong, "PLCN will significantly promote the competence of Hong Kong as a telecom hub in Asia-Pacific, offering sufficient capacity and faster route for internet and cloud services. . . . PLCN is changing internet and cloud connectivity in Hong Kong."[233] Here, PLCN would not be the only planned cable connecting the United States to Hong Kong; at least three additional applications for redundant cables to Hong Kong have been filed with the FCC since PLCN— the BtoBE cable (owners include Facebook, Amazon, and PRC state-owned carrier China Mobile);[234] the HKA cable (owners include Facebook and PRC state-owned carriers China Telecom and China Unicom);[235] and the Hong Kong-Guam cable (owners include Google and RTI).[236]

The Executive Branch has significant concerns that PLCN's proposed Hong Kong connection, combined with other pending applications seeking to directly connect the United States to Hong Kong, furthers the PRC's ambitions to have access to an information hub that is directly linked to U.S. ICT infrastructure. As stated in their application, the U.S. PLCN applicants' "respective affiliates [Google and Facebook] will use the PLCN capacity to connect their respective affiliates' data centers and POPs in the U.S. and Asia."[237] This proposed connection, coupled with the PRC's stated desire to use Hong Kong to "optimize the laying of

[233] Exhibit 85 at EB-PUBLIC-1427 to -28.

[234] *See* Exhibit 5 at EB-PUBLIC-53, *BtoBE Public Notice*. *See also supra* note 29.

[235] *See* Exhibit 6 at EB-PUBLIC-55, *HKA Public Notice*. *See also supra* note 29.

[236] *See* Exhibit 102 at EB-PUBLIC-1780, *HK-G Public Notice.* *See also supra* note 30.

[237] Exhibit 2 at EB-PUBLIC-7, *PLCN Application* at 3. *See also* Exhibit 3001 at CONF-GOOG-3 (originally produced as PLCN-001082) (Google's statement [redacted]).

submarine cable landing stations in China"[238] and its desire for what it terms to be "the most important connection direction for Internet services,"[239] potentially could place voluminous amounts of sensitive U.S. person data in these companies' possession at risk.

VI. If subject to appropriate mitigation, the Executive Branch recommends the Commission partially grant the license application for Google's and Facebook's connections between the United States, Taiwan, and the Philippines

If prior to the Commission issuing an order, PLCN's U.S. owners reach final agreements with the Team Telecom agencies on specific mitigation measures that address the Executive Branch's national security concerns relevant to those portions of the application, the Executive Branch recommends that the Commission partially grant Google and Facebook's application for a cable landing license to connect PLCN from the United States to Taiwan and the Philippines. The Executive Branch is sensitive to the need to use PLCN for commercial purposes in Taiwan and the Philippines. As such, it will continue to engage with Google and Facebook to tailor mitigation terms that are consistent with this recommendation, meet the interests of the United States in the foreign countries associated with this application, and address the United States' security interests.

VII. Conclusion

For the reasons stated above, the Executive Branch recommends that the Commission partially deny the PLCN cable landing license application with respect to PLCN's connection to Hong Kong and with respect to PLCN's foreign owners, Hong Kong-based Pacific Light Data Communication Co. Ltd. and China-based ultimate parent entity Dr. Peng Telecom & Media

[238] *See* Exhibit 36 at EB-PUBLIC-778 to 79, *CAICT White Paper* at 24-25.

[239] *See supra* note 228.

Group Co., Ltd. The Executive Branch further recommends that the Commission partially grant the license application for PLCN's U.S. owners GU Holdings, Inc. and Edge Cable Holdings USA, LLC, and for PLCN's connections between the United States, Taiwan, and the Philippines, subject to final mitigation agreements negotiated with the parties prior to the Commission issuing an order.

June 17, 2020

Respectfully submitted:

Kathy D. Smith
Chief Counsel

National Telecommunications and Information Administration

U.S. Department of Commerce Rm 4713
14th Street and Constitution Ave., N.W.
Washington, D.C. 20230
(202) 482-1816

CERTIFICATE OF SERVICE

I, Kathy Smith, herebv certify that on this 17th day of June, 2020, I caused a copy of the public inspection version of the Executive Branch Recommendation and exhibits to be served on the following via electronic mail. Those parties indicated with an "*" below also received a document describing the specific information withheld from public inspection for that party as well as the specific exhibits containing that party's business confidential information.

GU Holdings Inc.:
Austin Schlick*
Director, GU Holdings Inc.
25 Massachusetts Avenue NW, Ninth Floor
Washington, DC 20001
(202) 346-1100
schlick@google.com

Darah Franklin
Counsel, Google LLC
25 Massachusetts Avenue NW, Ninth Floor
Washington, DC 20001
(202) 346-1100
darahfranklin@google.com

Dan Brooks*
Nova Daley
Wiley Rein LLP
1776 K Street NW
Washington, DC 20006
NDaly@wileyrein.com
DBrooks@wileyrein.com

Todd Hinnen*
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
+1-206-359-8000
THinnen@perkinscoie.com

Edge Cable Holdings USA, LLC:
Johanna Ravelo
Associate General Counsel
Facebook, Inc.
One Hacker Way
Menlo Park, CA 94025-1452
+1 650 796 7804
jravelo@fb.com

Kent Bressie
Harris, Wiltshire & Grannis LLP
1919 M Street, N.W., Suite 800
Washington, D.C. 20036-3537
+1 202 730 1337
kbressie@hwglaw.com

Pacific Light Data Communication Co. Ltd:
Tsang, Yu Hoi*
Administration Manager
Unit 1705-1706, 17/F, One Peking, 1 Peking Road,
Tsim Sha Tsui, Kowloon, Hong Kong
+852 2682 6369
christsang@pldcglobal.com

Kathy Smith
Chief Counsel

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	File Nos.
GU HOLDINGS, INC.,	)	
EDGE CABLE HOLDINGS USA, LLC	)	SCL-LIC-20170421-00012;
and	)	SCL-AMD-20171227-00025;
Pacific Light Data COMMUNICATION	)	SCL-STA-20180907-00033;
CO. LTD.	)	SCL-STA-20190327-00011;
	)	SCL-STA-20190906-00032;
Application for a License to Construct, Land,	)	SCL-STA-20200129-00006;
and Operate an Undersea Fiber Optic Cable	)	SCL-STA-20200313-00014;
Connecting the United States, Hong Kong,	)	SCL-STA-20200402-00015.
Taiwan, and the Philippines	)	

Executive Branch Recommendation for a Partial Denial and Partial Grant of the Application for the Pacific Light Cable Network (PLCN) Cable Landing License

INDEX OF PUBLIC EXHIBITS

Ex. No.	Description	Start Page
004	TeleGeography, *Pacific Light Cable Network - PLCN*, Submarine Cable Map, https://www.submarinecablemap.com/#/submarine-cable/pacific-light-cable-network-plcn (last visited Mar. 21, 2020).	EB-PUBLIC-50
005	*Streamlined Submarine Cable Landing License Applications, Accepted for Filing,* Public Notice, Report No. SCL-00232S (Dec. 26, 2018) (hereinafter *BtoBE Public Notice*).	EB-PUBLIC-51
006	*Streamlined Submarine Cable Landing License Applications, Accepted for Filing,* Public Notice, Report No. SCL-00223S (Aug. 23, 2018) (hereinafter *HKA Public Notice*).	EB-PUBLIC-54
007	*Actions Taken Under Cable Landing License Act,* Public Notice, Report No. SCL-00193 (Jan. 13, 2017) (hereinafter *NCP Grant Public Notice*).	EB-PUBLIC-58
008	*Streamlined Submarine Cable Landing License Applications, Accepted for Filing,* Public Notice, Report No. SCL-00170S (Dec. 3, 2015) (hereinafter *NCP Public Notice*).	EB-PUBLIC-62
009	*Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference*, White House (Sept. 25, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.	EB-PUBLIC-66
010	*Fact Sheet: President Xi Jinping's State Visit to the United States,* White House (Sept. 25, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.	EB-PUBLIC-84
011	*G20 Leaders' Communiqué, Antalya Summit, 15-16 November 2015,* G20 (Nov. 16, 2015), https://www.consilium.europa.eu/media/23729/g20-antalya-leaders-summit-communique.pdf.	EB-PUBLIC-90
012	*Deputy Attorney General Rod J. Rosenstein Announces Charges Against Chinese Hackers,* U.S. Dep't of Justice (Dec. 20, 2018), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-announces-charges-against-chinese-hackers.	EB-PUBLIC-102

Ex. No.	Description	Start Page
013	*Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information,* U.S. Dep't of Justice (Dec. 20, 2018), https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.	EB-PUBLIC-104
014	*Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax,* U.S. Dep't of Justice (Feb. 10, 2020), https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking.	EB-PUBLIC-108
015	*Attorney General William P. Barr Announces Indictment of Four Members of China's Military Hacking into Equifax,* U.S. Dep't of Justice (Feb. 10, 2020), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military.	EB-PUBLIC-111
016	*United States v. Zhu Hua et al.,* Case No. 18-cr-891, Indictment (S.D.N.Y. filed Dec. 17, 2018)	EB-PUBLIC-113
017	*United States v. Wu Zhiyong et al.,* Case No. 20-cr-046, Indictment (N.D. Ga. filed Jan. 28, 2020)	EB-PUBLIC-136
018	*Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People,* U.S. Dep't of Justice (May 9, 2019), https://www.justice.gov/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including.	EB-PUBLIC-160
019	*United States v. Fujie Wang et al.,* No. 19-cr-153, Indictment (S.D. Indiana) (filed May 7, 2019).	EB-PUBLIC-163
020	Majority Staff Report, *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation,* Committee on Oversight and Government Reform, U.S. House of Representatives, 114th Cong. (Sept. 7, 2016).	EB-PUBLIC-180
021	David Sanger, *Marriott Concedes 5 Million Passport Numbers lost to Hackers Were Not Encrypted,* New York Times (Jan. 4, 2019), https://www.nytimes.com/2019/01/04/us/politics/marriott-hack-passports.html.	EB-PUBLIC-421

Ex. No.	Description	Start Page
022	Garrett M. Graff, *China's Hacking Spree Will Have a Decades-Long Fallout*, Wired (Feb. 11, 2020) https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/.	EB-PUBLIC-425
023	Ben Kochman, *Equifax Hack Shows China's Expanding Hunger for Data*, Law360, https://www.law360.com/cybersecurity-privacy/articles/1242594/equifax-hack-shows-china-s-expanding-hunger-for-data (Feb. 11, 2020)	EB-PUBLIC-431
024	CFIUS Reform: Examining the Essential Elements: Hearing on S. 2098 Before the S. Comm. on Banking, Hous., and Urban Affairs, 115th Cong. (2018) (excerpted).	EB-PUBLIC-434
025	Provisions Pertaining to Certain Investments in the United States by Foreign Persons, 84 Fed. Reg. 50174 (proposed Sept. 24, 2019) (codified at 31 C.F.R. pt. 800).	EB-PUBLIC-442
026	*National Security Strategy of the United States of America,* White House (Dec. 2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf.	EB-PUBLIC-480
027	2018 Report to Congress of the U.S.-China Economic and Security Review Commission, 115th Cong. 259 (2018) (Chapter 3, Section 1: Belt and Road Initiative), https://www.uscc.gov/sites/default/files/2019-09/2018%20Annual%20Report%20to%20Congress.pdf.	EB-PUBLIC-548
028	D. Kliman and A. Grace, *Power Play: Addressing China's Belt and Road Strategy*, Center for a New American Security 1 (Sept. 2018), https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-Power-Play-Addressing-Chinas-Belt-and-Road-Strategy.pdf?mtime=20180920093003.	EB-PUBLIC-602
029	*Assessment on U.S. Defense Implications of China's Expanding Global Access,* U.S. Dep't of Defense 12 (Dec. 2018).	EB-PUBLIC-646
030	DigiChina, *Translation: Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference,* New America (last visited Mar. 9, 2020), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/.	EB-PUBLIC-680

Ex. No.	Description	Start Page
031	Eric Rosenbach and Katherine Mansted, *The Geopolitics of Information,* Belfer Center, Harvard Kennedy School (May 28, 2019), https://www.belfercenter.org/publication/geopolitics-information.	EB-PUBLIC-689
032	Andrew Kitson and Kenny Liew, *China Doubles Down on Its Digital Silk Road,* Center for Strategic and International Studies (Nov. 14, 2019), https://reconnectingasia.csis.org/analysis/entries/china-doubles-down-its-digital-silk-road/.	EB-PUBLIC-705
033	Stacia Lee, *The Cybersecurity Implications of Chinese Undersea Cable Investment,* Univ. of Washington Jackson School of Int'l Studies (Feb. 6, 2017), https://jsis.washington.edu/eacenter/2017/02/06/cybersecurity-implications-chinese-undersea-cable-investment/.	EB-PUBLIC-719
034	Mark Zuckerberg, *Standing for Voice and Free Expression*, Facebook.com (Oct. 17, 2019), https://www.facebook.com/notes/mark-zuckerberg/standing-for-voice-and-free-expression/10157267502546634/.	EB-PUBLIC-727
035	Paul Triolo, Samm Sacks, Graham Webster, Rogier Creemers, China's Cybersecurity Law One Year On, New America (Nov. 30, 2017), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/.	EB-PUBLIC-740
036	*White Paper on China International Optical Cable Interconnection*, China Academy of Information and Communications Technology (Aug. 2018), http://www.caict.ac.cn/english/research/whitepapers/202003/P020200327550620516330.pdf (hereinafter *CAICT White Paper*).	EB-PUBLIC-749
037	Julia Voo, *A Case for Fortifying the BUILD Act: The U.S., China, and Internet Infrastructure in the Global South*, Belfer Center, Harvard Kennedy School (July 2019), https://www.belfercenter.org/publication/case-fortifying-build-act-us-china-and-internet-infrastructure-global-south	EB-PUBLIC-785
038	John Hemmings and Patrick Cha, *Exploring China's Orwellian Digital Silk Road,* The National Interest (Jan. 7, 2020), https://nationalinterest.org/feature/exploring-china%E2%80%99s-orwellian-digital-silk-road-111731.	EB-PUBLIC-800
039	*What is the OSI Model?*, Cloudflare, (last visited Mar. 2, 2020), https://www.cloudflare.com/learning/ddos/glossary/open-	EB-PUBLIC-807

Ex. No.	Description	Start Page
	systems-interconnection-model-osi/	
040	Jonathan E. Hillman, *Influence and Infrastructure: The Strategic Stakes of Foreign Projects,* Center for Strategic and Int'l Studies (Jan. 2019), https://www.csis.org/analysis/influence-and-infrastructure-strategic-stakes-foreign-projects	EB-PUBLIC-816
041	Murray Scot Tanner, *Beijing's New National Intelligence Law: From Defense to Offense,* Lawfare (July 20, 2017), https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.	EB-PUBLIC-849
042	Steve Dickinson, *China's New Cybersecurity Program: NO Place to Hide,* Harris Bricken (Sept. 30, 2019), https://www.chinalawblog.com/2019/09/chinas-new-cybersecurity-program-no-place-to-hide.html.	EB-PUBLIC-853
043	Rogier Creemers, Paul Triolo, and Graham Webster, *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)*, New America (June 29, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.	EB-PUBLIC-863
044	*White Paper: Implementing China's Cybersecurity Law,* Jones Day (Aug. 2017), https://www.jonesday.com/en/insights/2017/08/implementing-chinas-cybersecurity-law.	EB-PUBLIC-890
045	Paul Triolo, Samm Sacks, Graham Webster, Rogier Creemers, China's Cybersecurity Law One Year On, New America (Nov. 30, 2017), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/.	EB-PUBLIC-904
046	Katharine Tai, Lorand Laskai, Rogier Creemers, Mingli Shi, Kevin Neville, and Paul Triolo, *Translation: China's New Draft "Data Security Management Measures,"* (Draft for Comment), New America (May 31, 2019), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-draft-data-security-management-measures/.	EB-PUBLIC-913
047	Carolina Dackö and Lucas Jonsson, *Applicability of National Intelligence Law to Chinese and non-Chinese Entities,* Mannheimer Swartling (Jan. 2019), https://www.mannheimerswartling.se/globalassets/nyhetsbrev/msa_nyhetsbrev_national-intelligence-law_jan-19.pdf	EB-PUBLIC-925
048	*National Intelligence Law of the People's Republic,* National People's Congress, (last visited Mar. 24, 2020), https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf (Google's cache of	EB-PUBLIC-931

Ex. No.	Description	Start Page
	http://www.npc.gov.cn/npc/xinwen/2017-06/27/content_2024529.htm as it appeared on Mar. 25, 2019, 5:27:04 GMT).	
049	Murray Scot Tanner, *Beijing's New National Intelligence Law: From Defense to Offense,* Lawfare (July 20, 2017), https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.	EB-PUBLIC-937
050	Adam Satariano, *How the Internet Travels Across Oceans,* NYTimes.com (Mar. 10, 2019), https://www.nytimes.com/interactive/2019/03/10/technology/internet-cables-oceans.html.	EB-PUBLIC-940
051	Jayne Miller, *Want to Understand Content Providers' Priorities? Look at Where They're Building Cables,* TeleGeography (May 25, 2018), https://blog.telegeography.com/content-providers-google-submarine-cables-bandwidth-market-junior-curie.	EB-PUBLIC-950
052	Alan Weissberger, *Will Hyperscale Cloud Companies (e.g., Google) Control the Internet's Backbone?,* IEEE Communications Society (Apr. 25, 2019), https://techblog.comsoc.org/2019/04/25/will-hyperscale-cloud-companies-e-g-google-control-the-internets-backbone/.	EB-PUBLIC-954
053	Rich Miller, *Cloud Players are Redrawing the Subsea Cable Map*, Data Center Frontier (Dec. 4, 2018), https://datacenterfrontier.com/cloud-players-are-redrawing-the-subsea-cable-map/.	EB-PUBLIC-965
054	Vinay Nagpal and Erick Contag, *Convergence of Data Centers, Subsea, and Terrestrial Fiber*, Pacific Telecommunications Council (Sept. 19, 2019), https://www.ptc.org/20190/09/convergence-of-data-centers-subsea-and-terrestrial-fiber/.	EB-PUBLIC-981
055	Tim Stronge, Jon Hjembo, Brianna Boudreau, *TeleGeography at PTC 2020,* TeleGeography (Jan. 19, 2020), https://www2.telegeography.com/ptc-2020.	EB-PUBLIC-986
056	Brian Lavallée, *Connecting Data Centers Under the Sea, Ciena* (Apr. 27, 2016), https://www.ciena.com/insights/articles/Connecting-Data-Centers-Under-the-Sea_prx.html.	EB-PUBLIC-1057
057	Jeff Hecht, *The Bandwidth Bottleneck that is Throttling the Internet*, Nature (Aug. 10, 2016), https://www.nature.com/news/the-bandwidth-bottleneck-that-is-throttling-the-internet-1.20392	EB-PUBLIC-1065
058	Guy Matthews, *Power Beneath the Surface*, Capacity (Dec. 3, 2019), https://www.capacitymedia.com/articles/3824623/power-	EB-PUBLIC-1074

Ex. No.	Description	Start Page
	beneath-the-surface	
059	Jeff Hecht, *Submarine cable goes for record: 144,000 Gigabits from Hong Kong to L.A. in 1 Second*, IEEE Spectrum (Jan. 3, 2018), https://spectrum.ieee.org/telecom/internet/submarine-cable-goes-for-record-144000-gigabits-from-hong-kong-to-la-in-1-second.	EB-PUBLIC-1080
060	TeleGeography, *White Paper, Subsea cables and interconnection hubs: The interplay of diversifying routes and peering markets*, DE-CIX (Jan. 2019), https://www.de-cix.net/en/about-de-cix/academy/white-papers/subsea-cables-and-interconnection-hubs-the-interplay-of-diversifying-routes-and-peering-markets.	EB-PUBLIC-1087
061	Daniel S. Hamilton and Joseph P. Quinlan, *The Transatlantic Economy 2019,* Foreign Policy Institute (2019) (Chapter 3—From Pipes to Platforms: The Transatlantic Digital Economy), https://transatlanticrelations.org/wp-content/uploads/2019/03/TE2019_Chapter-3.pdf.	EB-PUBLIC-1100
062	Shreya Gautam, Ronald Rapp, Richard Kraum, Jonathan Liss, Richard Pierce, *Physical and Cyber Security for Undersea Cables in an Open Cable Environment,* SubOptic 2019 (2019)	EB-PUBLIC-1118
063	Drew FitzGerald, *Google, Facebook to Invest in U.S.-China Data Link,* Wall Street Journal (Oct. 12, 2016).	EB-PUBLIC-1124
064	Company Name Search, Integrated Companies Registry Information System (ICRIS), Companies Registry—Government of Hong Kong	EB-PUBLIC-1127
065	*Some Hong Kong companies change their name every couple months; Data Guru exposes the worst culprits*, dataguru.hk (Dec. 24, 2018), https://blog.dataguru.hk/2018/12/24/some-hong-kong-companies-change-their-name-every-couple-of-months-why/.	EB-PUBLIC-1131
066	*Name Change, Change of Stock Short Name and Company Website,* China Jinhai International Group Limited (Dec. 4, 2014), http://doc.irasia.com/listco/hk/centralwealth/announcement/a141204.pdf.	EB-PUBLIC-1139
067	*Name Change, Changes of Stock Short Name and Company Website,* China Soft Power Technology Holdings Limited (Aug. 13, 2015) http://doc.irasia.com/listco/hk/centralwealth/circulars/c150813.pdf .	EB-PUBLIC-1142

Ex. No.	Description	Start Page
068	*Name Change, Changes of Stock Short Names and Company Website,* Central Wealth Group Holdings Limited.	EB-PUBLIC-1145
069	Winston Qiu, *Invader to Build Pacific Light Cable Network Connecting Hong Kong and the US,* Submarine Cable Networks (Nov. 16, 2015), https://www.submarinenetworks.com/en/systems/trans-pacific/plcn/invader-to-build-pacific-light-cable-network-connecting-hong-kong-and-the-us.	EB-PUBLIC-1148
070	*Inside Information, Entering into the Memorandum of Understanding and the Professional Services Agreement*, China Soft Power Technology Holdings Limited (Nov. 13, 2015), https://doc.irasia.com/listco/hk/centralwealth/announcement/a151113.pdf	EB-PUBLIC-1153
071	Comms Update, *Cable Compendium: a guide to the week's submarine and terrestrial developments,* TeleGeography (Nov. 20, 2015), https://www.commsupdate.com/articles/2015/11/20/cable-compendium-a-guide-to-the-weeks-submarine-and-terrestrial-developments/.	EB-PUBLIC-1160
072	*Connected Transaction: Disposal of Entire Interest in PLD Holdings Limited*, China Soft Power Technology Holdings Limited (Mar. 31, 2016), https://doc.irasia.com/listco/hk/centralwealth/announcement/a160331.pdf.	EB-PUBLIC-1162
073	*Discloseable and Connected Transaction: Disposal of Entire Interest in CPST Holdings Limited, Proposed Re-election of Director and Notice of Special General Meeting*, China Soft Power Technology Holdings Limited (Aug. 3, 2016), https://doc.irasia.com/listco/hk/centralwealth/circulars/c160802.pdf	EB-PUBLIC-1169
074	*Offering Memorandum,* Dr. Peng Telecom & Media Group Co., Ltd. (May 25, 2017), https://links.sgx.com/FileOpen/DrPHHL_Offering%20Memorandum%20dated%2025%20May%202017.ashx?App=Prospectus&FileID=31941 (excerpts of relevant portions)	EB-PUBLIC-1203
075	Kate O'Keeffe, Drew FitzGerald, and Jeremy Page, *National Security Concerns Threaten Undersea Data Link Backed by Google, Facebook,* Wall Street Journal (Aug. 28, 2019)	EB-PUBLIC-1288

Ex. No.	Description	Start Page
076	*Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charged in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets,* U.S. Dep't of Justice (Feb. 13, 2020), https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-subsidiaries-charged-racketeering	EB-PUBLIC-1293
077	*United States v. Huawei Technologies Co., Ltd., et al.,* Cr. No. 18-457, ECF No. 126, Superseding Indictment (Feb. 13, 2020).	EB-PUBLIC-1296
078	*Entouch Systems, Inc. v. J. Lyn Findley,* C.A. No. 2018-0817-KSJM, Defendant's Answer, Affirmative Defenses, and Verified Counterclaim (Del. Ch. Ct. Jan. 14, 2019)	EB-PUBLIC-1352
079	*J. Lyn Findley v. enTouch Systems, Inc.,* Case No. 2018-65570, Plaintiff's Original Petition (Tex. Dist. Ct. filed Sept. 18, 2018)	EB-PUBLIC-1375
080	*Selected Application Listing By File Number*, FCC File Number ITC-214-19980226-00152, FCC International Bureau (last visited Mar. 18, 2020) (search for "Vertex Group ")	EB-PUBLIC-1408
081	Yongzhe Jin Profile, LinkedIn (last visited May 14, 2019), https://www.linkedin.com/in/yongzhe-jin-80b2b67/?originalSubdomain=cn.	EB-PUBLIC-1411
082	Troy Yunfeng Li Profile, LinkedIn (last visited May 14, 2019), https://www.linkedin.com/in/troy-yunfeng-li-07945456/.	EB-PUBLIC-1415
083	Eric Liu Profile, LinkedIn (last visited May 14, 2019), https://www.linkedin.com/in/eric-liu-47b10914/.	EB-PUBLIC-1418
084	Winston Qiu Profile, LinkedIn (last visited June 11, 2019), https://www.linkedin.com/in/winston-qiu-8946973b/.	EB-PUBLIC-1422
085	Winston Qiu, *Next Steps in the Pacific: A Subsea Cable Changing Internet and Cloud Infrastructure Across the Pacific,* Submarine Telecoms Forum 34 (May 2018)	EB-PUBLIC-1427
086	Winston Qiu, *PLCN, a subsea cable changing internet and cloud infrastructure across the Pacific,* Submarine Cable Networks (Jun. 28, 2018), https://www.submarinenetworks.com/en/systems/trans-pacific/plcn/plcn-a-subsea-cable-changing-internet-and-cloud-infrastructure-across-the-pacific.	EB-PUBLIC-1429
087	*Annual Report 2018,* PCCW (2018), http://www.pccw.com/staticfiles/PCCWCorpsite/About%20PCCW/Investor%20Relations/Announcements%20&%20Notices/2019/Apr/2018-pccw-annual-report.pdf	EB-PUBLIC-1438

Ex. No.	Description	Start Page
088	Qin Min and Zhao Runhua, *China's State-owned Carriers Edge Consumer Broadband Giant out of the Market,* Caixin Global (Apr. 2, 2019), https://www.caixinglobal.com/2019-04-02/chinas-state-owned-carriers-edge-consumer-broadband-giant-out-of-the-market-101400247.html	EB-PUBLIC-1666
089	Eric Handa, *Trans-Pacific Market Capacity: Innovating and Adapting in the Face of Challenges,* Submarine Telecoms Forum 36 (May 2019)	EB-PUBLIC-1670
090	Matt Burgess, *Google and Facebook are gobbling up the internet's subsea cables,* Wired UK (Nov. 18, 2018), https://www.wired.co.uk/article/subsea-cables-google-facebook	EB-PUBLIC-1677
091	Colin Anderson, *Retirement at Age 25? Extending Submarine Cable's Lifespan,* ISE Magazine (May 27, 2016), https://www.isemag.com/2016/05/retirement-at-age-25/	EB-PUBLIC-1684
092	*Intentionally skipped*	*n/a*
093	*Intentionally skipped*	*n/a*
094	Alan Mauldin, Is Your Planned Submarine Cable Doomed? TeleGeography, Submarine Networks World 2019 (Sept. 17, 2019), https://www2.telegeography.com/hubfs/2019/Presentations/Alan-Mauldin-Sub-Nets-World-2019.pdf.	EB-PUBLIC-1688
095	Alan Mauldin, Is Your Planned Submarine Cable Doomed? TeleGeography Blog, (Oct. 8, 2019) https://blog.telegeography.com/is-your-planned-submarine-cable-doomed.	EB-PUBLIC-1709
096	*Intentionally skipped*	*n/a*
097	Unauthorized Landing of Submarine Cables in the United States, H.R. Rep. No. 67-71 (May 1921)	EB-PUBLIC-1715
098	Submarine Cables, 1921 Cong. Rec. Senate 651, 655 (Apr. 26, 1921)	EB-PUBLIC-1719
099	*Streamlined Submarine Cable Landing License Applications, Accepted for Filing,* Public Notice, Report No. SCL-00204S (Nov. 1, 2017) (hereinafter *PLCN Public Notice*).	EB-PUBLIC-1726
100	Amendment to Application for a Cable Landing License, SCL-AMD-20171227-00025 (Dec. 27, 2017) (hereinafter *PLCN Application Amendment*).	EB-PUBLIC-1730
101	*Application for a Cable Landing License, Streamlined Processing Requested*, SCL-LIC-20170421-00012 (filed Apr. 21, 2017) (hereinafter *PLCN Application*).	EB-PUBLIC-1738

Ex. No.	Description	Start Page
102	*Streamlined Submarine Cable Landing License Applications, Accepted for Filing,* Public Notice, Report No. SCL-00256S (Dec. 27, 2019) (hereinafter *HK-G Public Notice*).	EB-PUBLIC-1780
103	*Third Supplement to Application for a Cable Landing License (Streamlined Processing Requested),* SCL-LIC-20170421-00012 (filed Oct. 26, 2017) (hereinafter *PLCN Application Third Supplement*).	EB-PUBLIC-1783
104	*Request for Special Temporary Authority,* SCL-STA-20200129-00006 (filed Jan. 29, 2020) (hereinafter *PLCN Commercial Operations STA*)	EB-PUBLIC-1796
105	*2015-16 Annual Report,* China Soft Power Technology Holdings Limited (June 22, 2016), https://doc.irasia.com/listco/hk/centralwealth/annual/2016/ar2016.pdf	EB-PUBLIC-1806
106	Winston Qiu, Dr. Peng Acquires PLCN（鹏博士发布收购PLCN海缆项目公告), Submarine Cable Networks (Dec. 11, 2017), https://www.submarinenetworks.com/zh/cables/dr-peng-acquires-plcn	EB-PUBLIC-1968
107	Announcement of Dr. Peng Telecom & Media Group Co., Ltd. On the Acquisition of Vertex and related companies by subsidiaries, 鹏博士电信传媒集团股份有限公司关于子公司收购Vertex(擎天电讯)及关联公司股权的公告, 163.com (Apr. 29, 2015), http://quotes.money.163.com/f10/ggmx_600804_1769743.html	EB-PUBLIC-1980
108	*FCC Form 499 Filer Database*, Vertex Telecom, Inc. (last visited Mar. 25, 2019) http://apps.fcc.gov/cgb/form499/499detail.cfm?FilerNum=824966	EB-PUBLIC-1991
109	*In the Matter of ETS Telephone Company, Inc., ETS Cablevision, Inc., En-Touch Holdings, LLC, and ACME Communications, Inc.,* WC Dkt. No. 17-94, IB File No. ITC-T/C/-20170407-00061 (filed Apr. 10, 2017) (relevant portions)	EB-PUBLIC-1993
110	Federal Corporation Information, Dr. Peng Holding Canada, Inc., Government of Canada (last visited Mar. 24, 2020) https://www.ic.gc.ca/app/scr/cc/CorporationsCanada/fdrlCrpDtls.html?corpId=10480975	EB-PUBLIC-1995

Ex. No.	Description	Start Page
111	Hong Kong Basic Law, Chapter 8 (last visited Mar. 24, 2020), https://www.basiclaw.gov.hk/pda/en/basiclawtext/chapter_8.html	EB-PUBLIC-1998
112	*China says Hong Kong courts have no power to rule on face mask ban,* Reuters (Nov. 18, 2019), https://www.reuters.com/article/us-hongkong-protests-npc/china-says-hong-kong-courts-have-no-power-to-rule-on-face-mask-ban-idUSKBN1XS2OV	EB-PUBLIC-2000
113	*BRIEF-Dr Peng Telecom and Media's unit to acquire Vertex Group and related companies,* Reuters (Apr. 30, 2015), https://www.reuters.com/article/idUSL4N0XR2K420150430	EB-PUBLIC-2003
114	*Entouch Systems, Inc. v. J. Lyn Findley,* C.A. No. 2018-0817-KSJM, Stipulation of Dismissal with Prejudice (Del. Ch. Ct. Feb. 26, 2020).	EB-PUBLIC-2005
115	*Beyond the Build: Leveraging the Cyber Mission Force,* Aspen Institute (July 23, 2015) (Transcript of statement by Adm. M. Rogers), http://aspensecurityforum.org/wp-content/uploads/2015/07/Beyond-the-Build-Leveraging-the-Cyber-Mission-Force.pdf.	EB-PUBLIC-2007
116	Hong Kong Basic Law, Chapters 1 and 2 (last visited Mar. 30, 2020), https://www.basiclaw.gov.hk/pda/en/basiclawtext/chapter_1.html and https://www.basiclaw.gov.hk/pda/en/basiclawtext/chapter_2.html	EB-PUBLIC-2045
117	Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger, H. Permanent Select Comm. on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, U.S. House of Representatives, 112th Cong. (Oct. 8, 2012).	EB-PUBLIC-2051
118	5G Security—Huawei Factsheet, U.S. Dept. of State (Dec. 2019), https://policystatic.state.gov/uploads/2019/12/5G-Myth_Fact4.pdf	EB-PUBLIC-2111
119	*U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage,* U.S. Dep't of Justice (Nov. 27, 2017), https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations	EB-PUBLIC-2114

Ex. No.	Description	Start Page
120	Chris Bing, *DOJ reveals indictment against Chinese cyberspies that stole U.S. business secrets*, CyberScoop (Nov. 27, 2017), https://www.cyberscoop.com/boyusec-china-doj-indictment/	EB-PUBLIC-2118
121	@AmbJohnBolton. "Today, @TheJustice Dept indicted hackers who conduct unprecedented intellectual property theft on behalf of the Chinese Ministry of State Security. We stand w/ allies & partners in calling out this shameful violation of the 2015-US-China Cyber Commitments." *Twitter* (Dec. 20, 2018, 10:55 a.m.), https://twitter.com/AmbJohnBolton/status/1075781730831876096.	EB-PUBLIC-2129
122	Ian Smith, *Bolton Confirms China Was Behind OPM Data Breaches,* FedSmith (Sept. 21, 2018), https://www.fedsmith.com/2018/09/21/bolton-confirms-china-behind-opm-data-breaches/.	EB-PUBLIC-2132
123	Jeff Hecht, Optical Labs Set Terabit Transmission Records, IEEE Spectrum (Apr. 14, 2020)	EB-PUBLIC-2134
124	The Sino-British Joint Declaration, United Kingdom of Great Britain and Northern Ireland and the People's Republic of China, Dec. 19, 1984, https://www.cmab.gov.hk/en/issues/joint.htm.	EB-PUBLIC-2139
125	Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China (effective July 1, 1997), https://www.basiclaw.gov.hk/en/basiclawtext/images/basiclaw_full_text_en.pdf;	EB-PUBLIC-2159
126	Natasha Khan and Eva Dou, *Beijing Asserts Power to Declare Emergency to Quell Hong Kong Unrest,* Wall Street Journal (Sept. 3, 2019), https://www.wsj.com/articles/beijing-asserts-power-to-declare-emergency-to-quell-hong-kong-unrest-11567509276.	EB-PUBLIC-2327
127	Rich Miller, *White Paper: Hyperscale Data Centers,* Data Center Frontier and Iron Mountain (Sept. 2019), https://datacenterfrontier.com/white-paper/hyperscale-data-centers-special-report/.	EB-PUBLIC-2332
128	China adopts decision to make Hong Kong national security laws, Xinhua (May 28, 2020), http://www.xinhuanet.com/english/2020-05/28/c_139096394.htm	EB-PUBLIC-2344

Ex. No.	Description	Start Page
129	*Only national security legislation can bring Hong Kong lasting security*, Xinhua (May 27, 2020), http://www.npc.gov.cn/englishnpc/c23934/202005/aaa0ccb8145c48b0adaf860b054360cf.shtml	EB-PUBLIC-2346
130	P.R.C. National People's Congress Proposal on Hong Kong National Security Legislation, U.S. Dep't of State (May 27, 2020) (Statement of Secretary of State Michael R. Pompeo), https://www.state.gov/prc-national-peoples-congress-proposal-on-hong-kong-national-security-legislation/.	EB-PUBLIC-2348
131	2020 Hong Kong Policy Act Report, U.S. Dep't of State (May 28, 2020), https://www.state.gov/2020-hong-kong-policy-act-report/	EB-PUBLIC-2352

INDEX OF PLCN APPLICANTS' CONFIDENTIAL EXHIBITS

Ex. No.	Description	Start Page
1001	May 2019 Responses to Triage Questions received from all PLCN Applicants (originally produced as PLCN-000356 to -384)	CONF-PLCN-ALL-1
1002	May 2019 Responses to Triage Questions received from all PLCN Applicants, Appendix 1 and 2 (System Line Diagram and Ownership) (originally produced as PLCN-000385 to -389)	CONF-PLCN-ALL-30

INDEX OF PACIFIC LIGHT DATA'S CONFIDENTIAL EXHIBITS

Ex. No.	Description	Start Page
2001	May 2019 Responses to Triage Questions received from all PLCN Applicants, Appendix 12 and 13, Pacific Light Data Communication Co., Ltd., Ownership Information and Personal Identifiable Information (originally produced as PLCN-000540 to -549)	CONF-PLDC-1
2002	May 2019 Responses to First Set of Follow-up Questions, Appendix B, PLDC List of Customers (originally produced as PLCN-000909)	CONF-PLDC-11
2003	Oct. 31, 2019 Email from Google forwarding PLDC Responses to Third Set of Follow-up Questions (originally produced as PLCN-000921 to -1070)	CONF-PLDC-12

INDEX OF GOOGLE'S CONFIDENTIAL EXHIBITS

Ex. No.	Description	Start Page
3001	Excerpt of slides, PLCN Briefing for Team Telecom, Google (Feb. 27, 2020) (originally produced as PLCN-001080).	CONF-GOOG-1